Departamento de teoría de la señal y comunicaciones

PROYECTO FIN DE CARRERA

ESTUDIO Y DISEÑO DEL ACCESO A LA RED EN ENTORNOS AEROPORTUARIOS MEDIANTE TECNOLOGÍA WiMAX

Autor: Javier Martínez Gordillo

Tutora: Ana García Armada

Leganés, octubre de 2012

Agradecimientos

A toda la gente de Indra, por su apoyo en la elaboración de este proyecto,

en especial a Belén, Antonio, Miguel y Edu.

A Ana, por su amabilidad e implicación como tutora.

A tod@s mis amistades y compañer@s de facultad,

gracias por haber hecho este camino mucho más ameno.

A mis padres Juan Manuel y Patrocinio y mi hermano Jorge,

por vuestra fe, apoyo y ánimos.

Sin vosotros hubiera sido imposible.

Título: Estudio y diseño del acceso a la red en entornos aeroportuarios mediante tecnología WiMAX

Autor: Javier Martínez Gordillo

Director: Ana García Armada

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 22 de Octubre de 2012 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de:

VOCAL

SECRETARIO PRESIDENTE

RESUMEN

En este proyecto final de carrera se aborda la creación y validación de diversos módulos en C++ de un prototipo de sistema de comunicaciones basado en el estándar WiMAX móvil 802.16e. Este prototipo será utilizado para realizar pruebas sobre la tecnología que deberá soportar el nuevo enlace de comunicaciones AeroMACS, descrito dentro del proyecto europeo SESAR para la unificación en la gestión del tráfico aéreo europeo. Este enlace será el encargado de prestar, en un futuro, las comunicaciones entre las aeronaves y las torres de control cuando dichas aeronaves se encuentren ubicadas en superficies aeroportuarias dentro del territorio europeo. Para ello, AeroMACS hará uso del canal radio y de la tecnología WiMAX, adaptándola a las peculiaridades que requieren las comunicaciones aeronáuticas, relacionadas con la seguridad y el uso de bandas de frecuencia específicas.

A lo largo del capítulo 1º expondremos las líneas maestras del proyecto europeo SESAR y el encuadre del prototipo dentro de él.

En el capítulo 2º expondremos las características principales de la tecnología WiMAX móvil que emplearemos para desarrollar los módulos del prototipo. También serán explicados los escenarios virtuales que emplearemos para validar el desarrollo del prototipo.

El prototipo emplea como base la implementación boc-WiMAX, proporcionada de forma gratuita por la empresa Bollaré Telecom en su página web. Esta implementación proporciona un ASN-GW (equipos encargados de interconectar la red WiMAX con la red IP y gestionar los recursos de dicha red), una estación base y una estación móvil basadas en la tecnología WiMAX, con unas funcionalidades muy básicas.

Partiendo de esta implementación inicial, comenzaremos un estudio pormenorizado de todas las funcionalidades que contiene. Este estudio se desarrolla y explica con detalle a lo largo del capítulo 3º.

Una vez analizadas las capacidades de las que dispone boc-WiMAX pasaremos a iniciar el desarrollo de los módulos QoS y Handover en los distintos elementos de la red que deben componer la arquitectura de comunicaciones. Estos módulos resultan imprescindibles para conseguir un prototipo de sistema de comunicaciones capaz de atender aeronaves, caracterizadas, entre otras muchas cosas, por su movilidad, la seguridad de sus transmisiones y por la necesidad de transmitir y recibir flujos de tráfico de datos con distintas calidades de servicio.

A lo largo del capítulo 4º se detalla el procedimiento seguido para elaborar el módulo QoS, siguiendo fielmente las directrices del estándar 802.16e. Se procede a realizar, de igual manera, la validación de dicho módulo creando un caso de uso en un entorno simulado.

Finalmente, a lo largo del capítulo 5º se procederá a indicar la metodología que fue empleada para desarrollar el módulo de Handover de acuerdo a las directrices del estándar WiMAX móvil 802.16e y las recomendaciones del Network WiMAX Forum (NWF). Una vez explicado el desarrollo de dicho módulo se procede a validarlo mediante un caso de uso simulado.

SUMMARY

This Master's Thesis copes with the implementation and validation of a mock-up platform of a brand new mobile communications System based on the IEEE 802.16e standard. Furthermore, it deals with the development of the particular software modules required. The language used was C++.

European funded SESAR project, aims to deliver and standardize a brand new data link for surface communications within the airports. This data link is not only for communications between the control tower and the aircrafts but also for ones related to air carriers and their fleet.

As previously stated, the work carried out here encompasses the development of a prototype to verify and validate the technology.

This document is divided in several sections.

The first chapter gives the global framework of SESAR project (Single European Sky ATM Research) and where the mock-up fits in it.

Chapter two gathers the main characteristics of mobile WiMAX technology that were considered for the developments. Besides, all the scenarios simulated to validate the developments carried out are explained.

The implementation of the mock-up started off with an available implementation of the WiMAX standard called 'boc-WiMAX' released by the French company 'Bollaré Telecom'. This implementation provides elements of the architecture such as the ASN-GW, a Base Station and a Mobile one. It's important to highlight that the functionality implemented by Bollaré of these three elements is very basic and limited according to the standard.

As a previous step, a traceability analysis of all the features supported by the standard and the ones included in the Bollaré implementation was performed. Further information on this is detailed in chapter three.

Two major gaps were identified after the analysis. There was no QoS (Quality of Service), neither HO (Hand Over) implemented. These are mandatory procedures because of the mobility of the aircrafts and the need to have means to guarantee service provisioning in ATC (Air Traffic Communications) and traffic differentiation. Besides, these procedures affect different elements of the architecture.

Chapter four gathers all the work done in order to implement the QoS module according to the profile documentation issued by the WiMAX Forum. Moreover, it presents a scenario simulated to assess and validate the development of the module.

Finally, across chapter five, the methodology followed to develop the handover module compliant to WiMAX Forum profile and the recommendations coming from the Network WiMAX Forum (NWF) is explained. Once ended up with the development part, a specific scenario was settled to validate the implemented module.

ÍNDICE DE CONTENIDOS

TABLAS

FIGURAS

1 INTRODUCCIÓN

1.1 Espacio único europeo

Contrariamente a EE.UU., Europa no posee un espacio único aéreo en el que la gestión de dicho espacio aéreo sea administrada a niveles europeos. Además, el espacio aéreo europeo se encuentra entre uno de los más grandes del mundo con unos 33,000 vuelos en los días de mayor congestión y una elevada densidad aeroportuaria. Estas evidencias convierten al control de tráfico europeo en un asunto de elevada complejidad.

El espacio único europeo es un ambicioso proyecto lanzado por la Unión Europea en 2004 para reformar la arquitectura de la gestión del tráfico aéreo en Europa.

Se propone para ello un enfoque legislativo y tecnológico para cumplir con las capacidades y necesidades futuras de seguridad a nivel europeo en lugar de un nivel local.

El espacio único europeo es el único camino para proporcionar un nivel de seguridad elevado, eficiente y uniforme sobre los cielos europeos.

Los objetivos fundamentales del proyecto pasan por:

a) Reestructurar el espacio aéreo europeo en función de los flujos de tráfico aéreo
b) Crear capacidades adicionales
c) Incrementar la eficacia total de los sistemas de gestión de tráfico aéreo

La mayoría de los elementos de este nuevo marco de trabajo para la gestión del tráfico aéreo en Europa consisten en:

a) Separación de las actividades regulatorias de los servicios de provisión, posibilitando servicios de gestión aéreos transfronterizos.
b) Reorganizar el espacio europeo sin que este esté constreñido por las fronteras de cada estado miembro.
c) Establecer reglas y estándares comunes, cubriendo un amplio rango de problemas como el intercambio da datos de vuelo y las telecomunicaciones.

1.2 ¿Qué es SESAR?

SESAR (*Single European Sky ATM Research*) representa la dimensión tecnológica del cielo único europeo. Ayudará a crear un cambio en el paradigma actual de la gestión de los cielos europeos apoyándose en tecnologías innovadoras.

El programa SESAR aportará a Europa unas infraestructuras punteras e innovadoras para la gestión del control de tráfico aéreo que permitirán el desarrollo seguro y ecológico del transporte aéreo.

El fundamento del programa SESAR pasa por eliminar el enfoque fragmentado del ATM (*Air Traffic Management*), transformando el sistema actual, sincronizando todas las partes interesadas y los recursos federados. Por primera vez, todos los actores de la aviación europea están involucrados en la definición, desarrollo e implementación de un proyecto modernizador para la gestión del tráfico aéreo.

SESAR tiene como objetivo desarrollar una nueva generación de sistemas de gestión de tráfico aéreo capaces de garantizar un transporte aéreo mundial fluido y seguro durante los próximos 30 años. Está compuesto por tres fases:

1.- Fase de definición (2004-2008): Elaboración y entrega del plan maestro ATM en el que se definan los planes de contenido, desarrollo y despliegue de la nueva generación de sistemas ATM

2.- Fase de desarrollo (2008-2013): Producirá la tecnología, los componentes y los procedimientos operacionales detallados por el plan maestro definido en la fase 1ª para la consecución de los sistemas ATM de nueva generación.

3.- Fase de despliegue (2014-2020): Comprende la producción a gran escala y la implementación de la nueva infraestructura de gestión de tráfico aéreo compuesta por componentes de alto rendimiento, totalmente armonizados e interoperables que garanticen las actividades del transporte aéreo en Europa.

1.3 Fases de desarrollo

El programa SESAR se encuentra desglosado en su fase de desarrollo en 16 actividades operacionales diferenciadas, establecidas en 16 proyectos agrupados en cuatro aéreas de interés. A continuación presentaremos un listado con los 16 proyectos existentes y pasaremos posteriormente a detallar el WP15, dentro del cual se encuentra la actividad de nuestro proyecto.

a) Actividades Operacionales

- WP4.- Operaciones en ruta
- WP5.- Operaciones terminales (aterrizaje y despegue)
- WP6.- Operaciones Aeroportuarias
- WP7.- Operaciones de red
- WPE.- Largo plazo e investigación innovadora

b) Actividades de sistema de desarrollo

- WP9.- Sistemas de aeronave
- WP10.- Sistemas ATC (*Air Traffic Control*) en ruta y de aproximamiento
- WP11.- Servicios meteorológicos en vuelo
- WP12.- Sistemas aeroportuarios
- WP13.- Sistemas de información de gestión de red
- WP15.- Sistemas CNS (*Communications, Navigation & Surveillance*) no aviónicos

c) Gestión de sistemas de información

- SWIM.- Conectando el mundo ATM
- WP8.- Gestión de información
- WP14.- Arquitectura SWIM (*System Wide Information Management*)

d) Actividades transversales

- WP16.- I+D areas transversales
- WP3.- Validación de la adaptación e integración de la infraestructura
- WPB.- Arquitectura de mantenimiento
- WPC.- Plan maestro de mantenimiento

WP15.- Sistemas CNS no aviónicos

Este paquete de trabajo engloba un conjunto de proyectos cuya misión es establecer y realizar las fases de implementación y validación de las tecnologías CNS (*Communications, Navigantion & Surveillance*), considerando las compatibilidades pertinentes para prestar servicio a los usuarios de la aviación general como a la aviación militar. Identifica y define los sistemas para el futuro enlace de datos móvil que deberá prestar los servicios de comunicación y supervisión desde tierra. Proporciona la mejor combinación de tecnologías GNSS (*Global Navigation Satellite System*) y no-GNSS encargadas de dar soporte a los requerimientos.

Dentro de este conjunto de proyectos, nos centramos en aquellos englobados dentro de la categoría 15.2.X y mas concretamente en el 15.2.7, dentro del cual queda enmarcado el trabajo desarrollado que será expuesto en este proyecto.

Los proyectos de la categoría 15.2.X se encargan de definir la tecnología que dará soporte a los distintos *data links* (superficie, terrestre y satelital) que permitirán conectar la infraestructura terrestre de comunicaciones (SWIM) con las aeronaves y sus distintas fases de vuelo.

15.2.7.- *Data link* de superficie aeroportuario

SESAR 15.2.7 trata de desarrollar un nuevo sistema y un perfil de certificación para la especificación de características que deben ser implementadas en el futuro *data link* de servicios aeroportuarios en superficie. El perfil desarrollado, denominado AeroMACS, identificará el soporte de cada una de las características basadas en las especificaciones del estándar IEEE 802.16e. Con el objetivo de conseguir una estandarización con los procedimientos y metodologías existentes, AeroMACS se derivará del perfil C definido por el WiMAX Forum. Finalmente AeroMACS será validado mediante un prototipo que será puesto a prueba en los aeropuertos de Madrid-Barajas y Toulousse.

En la Figura 1 podemos observar la ubicación del proyecto 15.2.7 dentro de todos los proyectos que definirán la arquitectura de comunicaciones, tanto civiles como militares, del programa SESAR.

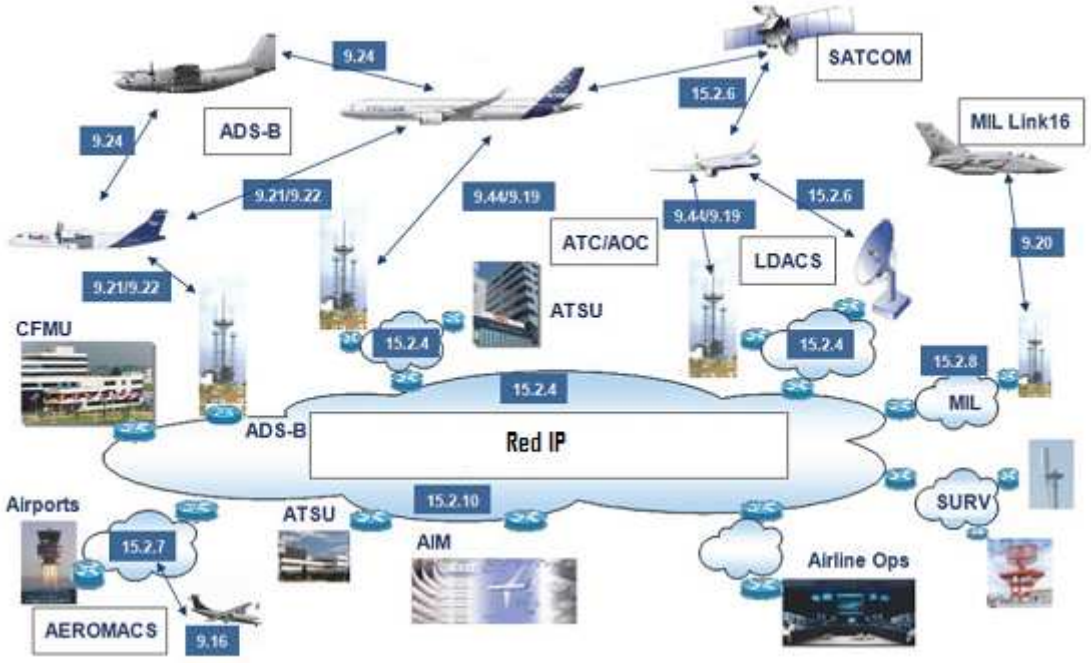


Figura 1 Proyectos SESAR involucrados en el despliegue de distintos enlaces de datos [8]

Una vez planteado el entorno en el que se ubica nuestro trabajo podemos proceder a plantear los objetivos de dicho trabajo.

Dentro del futuro enlace AeroMACS podremos encontrar tres actores bien diferenciados:

- MS (*Mobile Station*)
- BS (*Base Station*)
- ASN – GW (*Access Service Network-Gateway*)

Las estaciones móviles se encontrarán ubicadas en las aeronaves. Las estaciones base serán desplegadas por la superficie de los aeropuertos de tal forman que otorguen una cobertura y un ancho de banda suficiente para que las estaciones móviles soporten el conjunto de servicios operacionales definidas por las autoridades de navegación aérea aplicando políticas de *QoS* (*Quality of Service*). Por último cada aeropuerto contará con un único ASN. Este elemento será el encargado de mantener la visión global de la red establecida en el aeropuerto, servir de pasarela entre la red y el exterior y llevar la lógica de control en la red de acuerdo al perfil C definido por el WiMAX Forum.

Dentro de las muchas tareas que dicho ASN deberá gestionar, junto con las BSs, se encuentran la política QoS y el HO (*Handover*).

El perfil AeroMACS requiere entre otras muchas funcionalidades dos características fundamentales, *QoS* y *Handover*. En la actualidad, en el equipamiento comercial aún no se dispone de elementos que

posibiliten el *Handover* entre estaciones base y la implementación de la *QoS* se haya muy poco madura. Por todo ello, nuestro objetivo pasará por implementar estas funcionalidades dentro de un entorno de simulación de la arquitectura de red que deberá soportar el *datalink* AeroMacs. Dentro de la complejidad que dicho trabajo lleva implícita, nos centraremos en cubrir dichas funcionalidades a nivel lógico en la interfaz R6 (interfaz entre BSs y ASN), realizando una simplificación al mínimo de dichas funcionalidades en la interfaz R1 (interfaz radio) que nos permita validar los progresos realizados en la interfaz R6.

Empezaremos nuestro trabajo partiendo de un *software* libre descargado desde http://opensource.bolloretelecom.eu/projects/boc-WiMAX/ [9]. En dicha URL, la compañía *Bollere Telecom* nos brinda de forma totalmente gratuita el código fuente de una estación base, una estación móvil y un ASN WiMAX.

Nuestra primera tarea consistió en identificar y documentar las funcionalidades que este código libre proporcionaba, de acuerdo a las especificaciones establecidas por el WiMAX Forum, así como implementar un entorno de trabajo donde poder ejecutar el código. Dicho entorno se compondrá de máquinas virtuales, las cuales se encontrarán ubicadas en un servidor físico, que emularán los elementos de la arquitectura de red anteriormente citados: BSs, Mss y ASN.

2 ENTORNO DE TRABAJO

En este segundo capítulo empezaremos con una breve reseña sobre la tecnología WiMAX para, posteriormente, explicar el perfil WiMAX escogido en el radioenlace AeroMACS así como sus características. Este será el perfil que trataremos de emular en los despliegues de red que tengamos que realizar para validar los desarrollados realizados a lo largo del proyecto.
A continuación introduciremos los distintos escenarios implementados en el proyecto para desarrollar y validar los nuevos módulos de HO y QoS insertados en la implementación *boc-WiMAX*.
También describiremos cada uno de los actores que figuran en nuestros escenarios de red así como la utilidad de cada uno de ellos.

2.1 ¿Qué es WiMAX?

WiMAX, siglas de *Worldwide Interoperability for Microwave Access* (Interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 Ghz.

Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. El estándar que define esta tecnología es el IEEE 802.16.

El único organismo habilitado para certificar el cumplimiento del estándar y la interoperabilidad entre equipamiento de distintos fabricantes es el WiMAX Forum: todo equipamiento que no cuente con esta certificación, no puede garantizar su interoperabilidad con otros productos.

Actualmente se recogen dentro del estándar 802.16, existen dos variantes:
Uno de acceso fijo, (802.16d), en el que se establece un enlace radio entre la estación base y un equipo de usuario situado en el domicilio del usuario. Para el entorno fijo, las velocidades teóricas máximas que se pueden obtener son de 70 Mbps con un ancho de banda de 20 MHz. Sin embargo, en entornos reales se han conseguido velocidades de 20 Mbps con radios de célula de hasta 6 Km, ancho de banda que es compartido por todos los usuarios de la célula.
Otro de movilidad completa (802.16e), que permite el desplazamiento del usuario de un modo similar al que se puede dar en GSM/UMTS. Esta variante es la base del radio enlace AeroMACS.

Algunas de las principales características de la tecnología WiMAX son:

- Distancias de hasta 80 Km, con antenas muy direccionales y de alta ganancia.
- Velocidades de hasta 75 Mbps, 35+35 Mbps, siempre que el espectro esté completamente limpio.
- Facilidades para añadir más canales, dependiendo de la regulación de cada país.
- Anchos de banda configurables y no cerrados, sujetos a la relación de espectro.
- Permite dividir el canal de comunicación en pequeñas subportadoras (dos tipos: guardias y datos).

2.2 Perfil WiMAX Implementado

WiMAX Forum propone tres tipos de perfiles de funcionamiento diferentes a la hora de implementar una arquitectura de red basada en la tecnología WiMAX [2], perfil A, B y C. Antes de centrarnos en el perfil C, el cual implementará AeroMACS, mostramos en la Figura 2 el esquema de red generalizado de una arquitectura WiMAX.

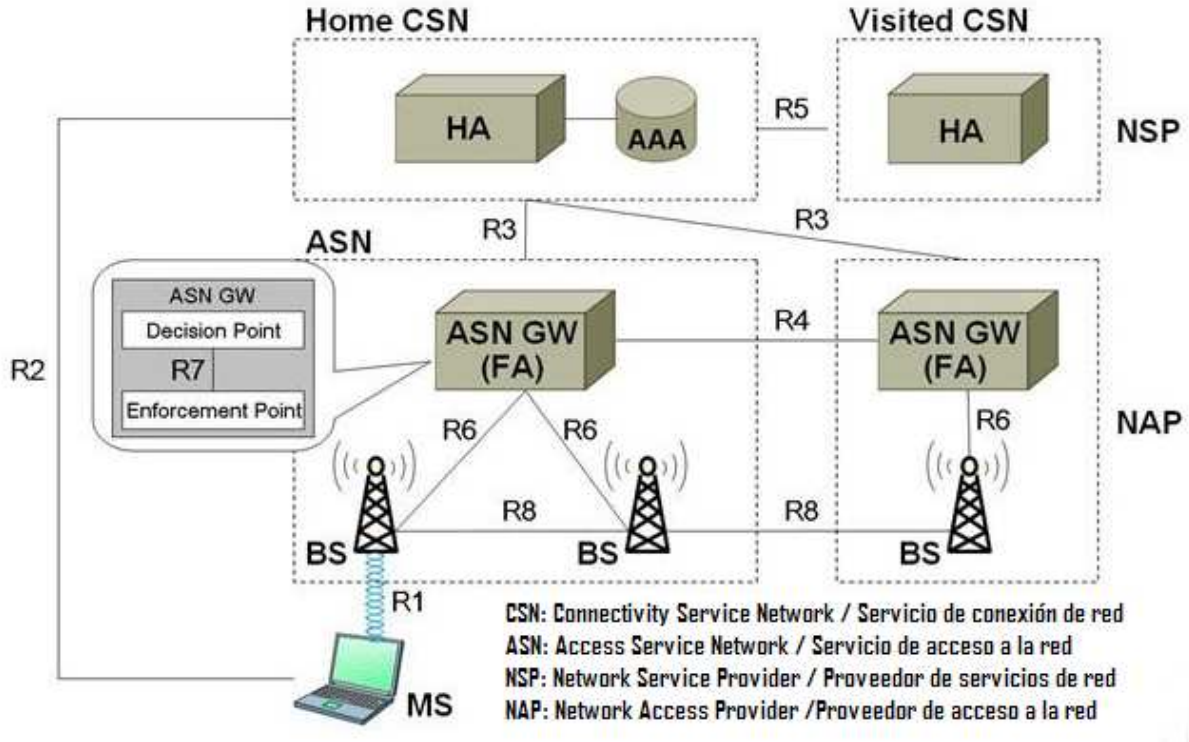


Figura 2 Arquitectura genérica de red WiMAX

En la Tabla 1 se muestran los interfaces definidos por el NWF (*Network WiMAX Forum*) para una red WiMAX.

Interfaces de red WiMAX	
R1	Interfaz inalámbrico encargado de conectar las estaciones móviles con las BS. Implementado en el estándar 802.16e
R2	Interfaz lógico entre CSN y MSs. Posibilita Mobile IP
R3	Interfaz definido entre ASN y CSN (*Connectivity Service Network*). Todos los mensajes radius y dhcp pasan a través de él.
R4	Interfaz lógico entre ASNs. Posibilita el HO durante el proceso de *Roaming*
R5	Interfaz entre *home* CSN y *visited* CSN. Usado en escenarios de *Roaming*
R6	Interfaz físico o lógico entre ASN y BSs. Posibilita Handoffs y RRM (*radio recurse managment*) así como todos los intercambios de información necesarios para la correcta entrada y salida en la red por parte de las MS
R7	Interfaz físico o lógico entre el punto de decisión y el punto de aplicación. Implementado en el ASN
R8	Interfaz lógico entre BSs. Usado durante el proceso de Handover (Haciendo uso de funcionalidades RRM)

Tabla 1 Interfaces WiMAX

Una vez que tenemos una visión global de la arquitectura genérica de una red WiMAX pasamos a mostrar las peculiaridades que presenta la arquitectura de red definida por el perfil C del NWF. Este perfil será el empleado en la arquitectura que deberá soportar el *data link* AeroMacs y sobre el cual implementaremos y probaremos los módulos de HO y QoS que desarrollemos.

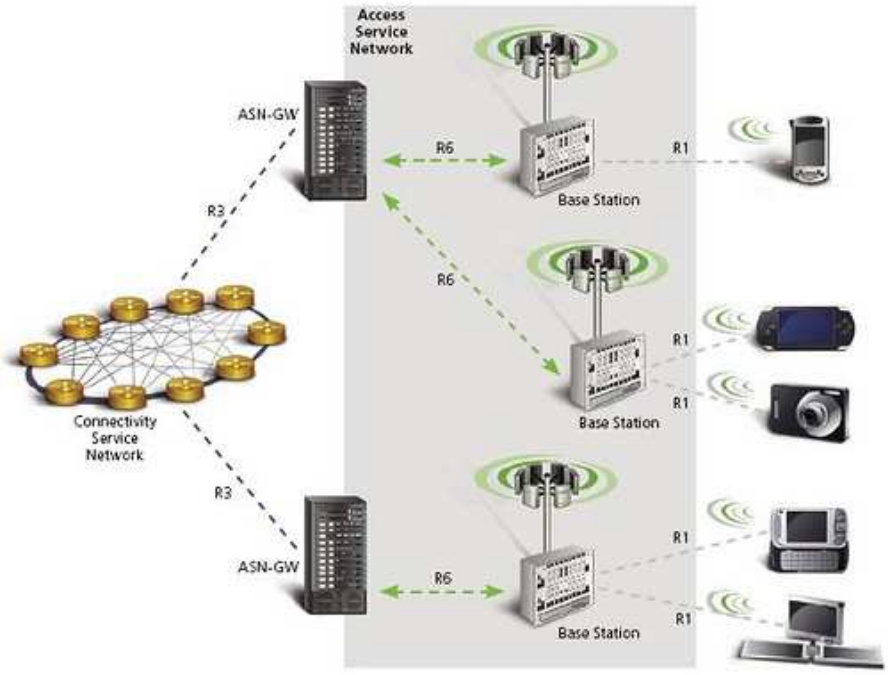


Figura 3 Arquitectura de red WiMAX perfil C

En la figura podemos comprobar como las únicos interfaces abiertas son el R1, R3, R4 y R6.

Dos características definen las principales ventajas de la adopción del perfil C. En primer lugar, en este perfil, las funcionalidades relacionadas con el canal radio (RRM y HO) se alejan completamente del ASN. El ASN toma el papel de elemento de interconexión, gestionando la lógica de red, mientras las BSs se quedan con toda la lógica asociada al canal radio.

En segundo lugar, el interfaz R6 queda definido como interfaz abierto.

Estas características aportadas por el perfil C resultan fundamentales a la hora de garantizar la interoperabilidad entre distintos proveedores y fabricantes ya que la comunicación entre BSs y ASNs queda estandarizada y las funciones de radio y red completamente separadas. Esta es la principal razón de la aplicación del perfil C WiMAX en el *data link* AeroMACS, garantizar la interoperabilidad entre distintos fabricantes en el despliegue de este nuevo canal de comunicaciones aeroportuarias.

Este fenómeno conlleva un cambio de enfoque bastante importante. Ahora las BSs no poseen ningún mecanismo para intercambiar información directamente entre ellas. Toda comunicación entre BSs debe hacerse pasando antes por el ASN, enviando la información por los interfaces R6. Ahora el ASN el elemento central de la red.

Esta elección marcará en gran medida la forma en que desarrollamos en módulo de HO, la cual será descrita con detalle en el capítulo 5º.

Por otro lado en nuestra implementación tampoco contemplamos la opción de habilitar servicios de *Roaming* ni *Mobile IP* ni funcionalidades RRM, con lo cual se prescinde de los interfaces R8, R5, R4 y R2.

Tampoco queda habilitado el interfaz R7.

2.3 Entidades participantes en el despliegue la red WiMAX simulada

Una vez que hemos descrito la arquitectura de red sobre la que implementaremos los módulos de HO y QoS, podemos pasar a explicar los distintos actores que tendrán que estar presentes en dicha arquitectura.

Para poder simular una red WiMAX de forma realista y realizar pruebas y validaciones sobre ella necesitaremos contar con las siguientes entidades:

- Servidor DHCP (*Dynamic Host Configuration Protocol*): Servidor encargado de proporcionar una dirección IP a cada uno de los CPE (*Customer Premises Equipment*) que deseen acceder a la red. El papel de este servidor es fundamental ya que con su acción se permite que los distintos CPE puedan obtener conectividad a nivel de red, el cual, es el objetivo último del establecimiento de la conexión.

En nuestra red, el servidor DHCP elegido fue el *dnsmasq*. Dnsmaq es un servidor de reenvío DNS (*Domain Name System*) y servidor DHCP. La facilidad que presenta a la hora de ser configurado y el poco espacio en memoria que requiere nos hicieron decantarnos por su elección. Este servidor puede ser descargado de forma gratuita para sistemas operativos UNIX bajo licencia GNU [3].

La versión instala de *dnsmasq* fue la 2.52. Debemos tener en cuenta que necesitamos instalar una versión superior a la 2.42. Es a raíz de dicha versión cuando *dnsmasq* comienza a soportar la extensiones del protocolo DHCP definidas por la RFC 3046 [4], en las que se define la mensajería y los

procedimientos necesarios para posibilitar la opción de un agente de retransmisión de información DHCP dentro de la red (el ASN en nuestro caso).

- Servidor AAA (*Authentication, Authorization & Accounting*): Dentro de la red, necesitamos disponer de un servidor AAA encargado de posibilitar la autenticación y autorización de los CPE que deseen acceder a la red. Dicho servidor contendrá la clave compartida asociada a cada uno de los CPE a partir de la cual se podrán autenticar. Contendrá además la MSK (*Master Session Key*), la información de todos los SF (*Service Flows*) que puede disponer cada uno de los dispositivos móviles conectados a la red así como las políticas de QoS asociadas a cada uno de los SF. Para más detalles acerca del uso y empleo de SFs ver el punto 4.3.2.

Debido a que el protocolo definido en las especificaciones del WiMAX Forum es el protocolo radius [5], debemos emplear un servidor AAA radius que soporte dicho protocolo. El servidor escogido fue *freeradius* también de *software* libre bajo licencia GNU [6].

La versión instalada de dicho servidor fue la 2.1.8. Debemos tener una versión instalada superior a la 2.1. Es a partir de dicha versión cuando queda implementado el módulo WiMAX dentro del servidor AAA. Dicho modulo implementa las especificaciones definidas por el WiMAX Forum [5] para establecer el formato y los procedimientos de intercambio de los AVPs [*Atribute Value Pairs*] a emplear cuando usemos el protocolo radius en combinación con la tecnología WiMAX.

- ASN-GW: El ASN-GW es el elemento capital dentro de la red. Su misión principal es realizar la tarea de pasarela entre el servidor AAA, el servidor DHCP, las BSs y las MSs. Este ASN funcionará bajo las directrices del perfil C WiMAX propuesto por el WiMAX Forum. Debemos recordar que este perfil propone un modelo de red centralizado en el ASN el cual posee gran parte de la lógica de control de la red.

Las funciones que el ASN-GW debe controlar pueden resumirse en:

- *Network Discovery* y selección del CSN/NSP (Connectivity Service Network/Network Service Provider) preferido
- Entrada en la red de acuerdo al estándar 802.16e basada en el establecimiento de conectividad a nivel MAC a través de un proxy AAA.
- Función de retransmisión a nivel IP
- Control de tráfico multicast y broadcast
- Movilidad intra-ASN (HO)
- Movilidad Inter-ASN (Roaming)
- Asistencia en la contabilidad de los recursos consumidos
- Redirección de datos
- Autorización de flujos de servicio (SFs)
- QoS
- Control de admisión & *Policing*

En nuestro despliegue, sólo tres de estas funciones serán obviadas. El ASN no tendrá que seleccionar entre distintos CSN/NSP puesto que se supone la existencia de un único CSN. En el despliegue de AeroMacs en los aeropuertos sólo se contara con un único proveedor de servicio en cada uno de ellos. Tampoco queda implementada la función de movilidad entre ASNs. En los aeropuertos existirá un único ASN y la opción de prestar servicios de *roaming* no queda contemplada. Por último, nuestro ASN tampoco realizará un control sobre los recursos consumidos por cada uno de los usuarios por simplicidad.

- BS: Presenta el objetivo de ser el nexo de unión entre la red y la interfaz radio. Presta cobertura a las MS y gestiona la ocupación del canal radio para cada una de las MSs a las que atiende.

- MS: Dispositivo terminal. En ella se ubica el código fuente correspondiente a la estación móvil, un cliente EAP y el cliente DHCP, concretamente el cliente udhcpc.

2.4 Escenarios de red implementados

En este apartado vamos a explicar los dos escenarios de red que han sido desplegados para validar las distintas funcionalidades que han sido añadidas al software *boc-WiMAX*.

2.4.1 Escenario básico

Escenario desplegado en primera instancia. Su misión es proporcionar la infraestructura necesaria para poder en funcionamiento todos los agentes descritos en el apartado 2.2 obteniendo conectividad a nivel MAC/IP entre ellos. Con este mismo escenario realizaremos la validación de las funcionalidades básicas del módulo de QoS implementado, ver capítulo 4º.

Para el despliegue de este escenario hacemos uso del software de virtualización *VMware* [7]. Este software funciona como una aplicación cliente-servidor. En el servidor se encuentran los recursos de memoria y procesamiento. Haciendo uso de estos recursos, podemos crear máquinas virtuales mediante el cliente (vSphere) de virtualización. Estas máquinas serán el núcleo básico de trabajo. Cada una de ellas posee un sistema operativo propio y funcionan como máquinas totalmente independientes a las que podemos añadir todos los elementos hardware que queramos de forma emulada.

El sistema operativo instalado en las máquinas virtuales fue Ubuntu, basado en el núcleo Linux. Trabajamos con las versiones *Hardy* y *Lucid*.

Para este escenario fue necesario el empleo de 4 máquinas virtuales:

- ASN-GW_v2: Esta máquina cumplió la función de ASN. En ella se compila el ejecutable correspondiente al ASN-GW. Distribución instalada: Ubuntu Hardy

- TelMAXVM_1: Esta máquina cumplirá la función de estación base y también contendrá el servidor AAA. En ella se copia el código fuente del proyecto boc-WiMAX correspondiente a la estación móvil. Distribución instalada: Ubuntu Lucid

- TelMAXVM_2: Esta máquina cumplirá las funciones de estación móvil, también se ubica en ella el cliente DHCP udhcpc. Distribución instalada: Ubuntu Lucid

- VM3: Esta máquina cumplirá las funciones de servidor DHCP. Para ello instalamos en ella el sofware dnsmasq. Distribución instalada: Ubuntu Hardy

Todas las máquinas son configuradas en el cliente vSphere para pertenecer a la misma subred. De esta forma el tráfico multicast que generemos en una de las máquinas, será recibido por todas las demás. Para darles salida al exterior conectaremos todas ellas a un switch virtual, el cual reencamirá el tráfico hacia un router. En la Figura 4 mostramos esta configuración de forma gráfica. Podremos apreciar que en la misma subred aparecen adicionalmente las máquinas boc-WiMAX_support1 y 2. Estas máquinas serán empleadas en posteriores escenarios.

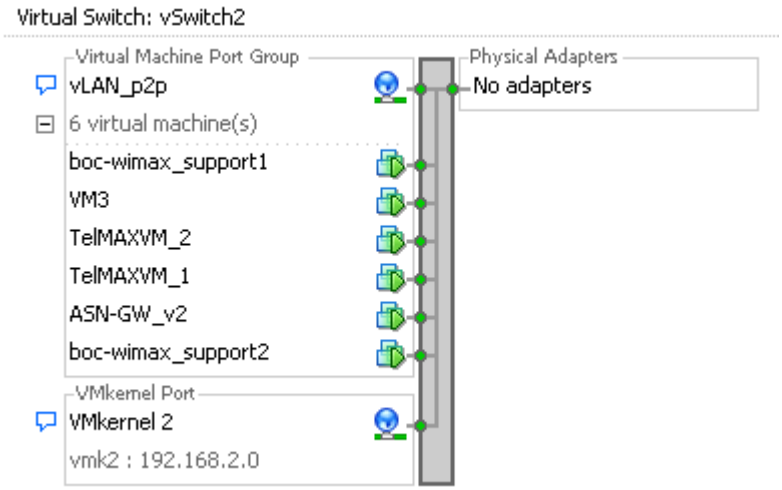


Figura 4 Configuración de red aplicada en VMWare

Mostramos seguidamente, en la Figura 5, el esquema de red implementado en el escenario básico, con todos los agentes involucrados.

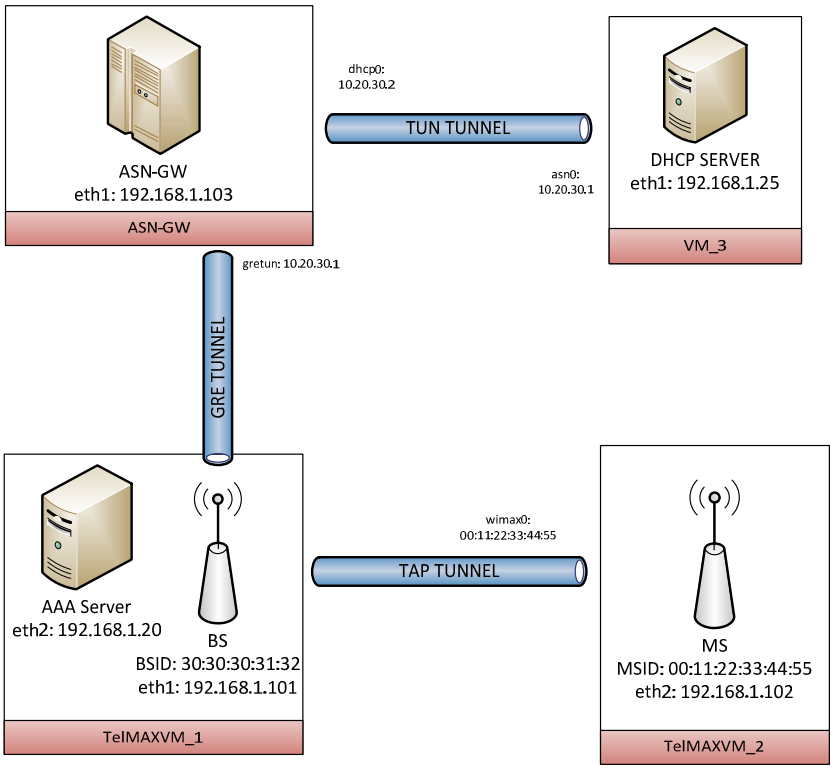


Figura 5 Esquema de red, escenario básico (tras el acceso a la red)

En la figura observamos la existencia de tres tipos de túneles diferentes que unen los distintos actores existentes en la red. Pasamos a explicar la función de cada uno de ellos:

- Túnel TAP: Túnel de nivel 2. Gestiona paquetes a nivel Ethernet. Se encuentra establecido entre los interfaces virtuales creados en las máquinas TelMAXVM_ 1 y TelMAXVM_2. Une, punto a punto, las direcciones MAC definidas por la MSID (asociada a la interfaz WiMAX0) y el BSID. Por tanto, todo el tráfico generado entre la MS se enviará a la BS vía túnel TAP. Este túnel trata de emular la conectividad a nivel MAC que existiría en el interfaz radio. Trata de hacer la conexión entre BS y MS transparente a nivel de red. También nos aporta la ventaja de poder tener varias IP con una única tarjeta de red, ya que para la simulación, necesitaremos crear la interfaz WiMAX0 aparte del interfaz de red que posea la máquina.

- Túnel TUN: A pesar que la MS pueda cambiar de ubicación y por tanto de punto de unión a Internet, surge la necesidad de mantener su IP una vez que se ha establecido la conexión a nivel de red, permitiendo adicionalmente la movilidad de dicha MS entre distintos puntos de acceso a la red. Para ello, debemos recurrir a técnicas de tunelado. El NWF propone dos alternativas para enlazar el ASN-GW con el HA (*home-agent*) del CSN a través del interfaz R3 [2]:

    a) Encapsulado IP sobre IP.- Solución elegida en la implementación *boc-WiMAX*. La encapsulación se realiza mediante un túnel TUN de acuerdo a la RFC 2003.

    b) Encapsulado GRE

- Túnel GRE (Generic Routing Encapsultation): GRE es un protocolo definido por la RFC2784 y extendido en la RFC2890. Nos sirve para realizar encapsulado IPoIP y discernir (en la BS) hacia que MS va dirigido el tráfico recibido del ASN-GW. Este protocolo presenta un campo denominado "key "donde mapearemos el Data-PathID a partir del cual queda identificada la estación móvil a la que va dirigida el tráfico, ver apartado 4.3.2.

Finalmente mostramos la torre de protocolos del plano de datos donde terminamos de comprender la utilidad de túneles explicados anteriormente. El túnel TUN se establece entre la interfaz R3, el GRE sobre la interfaz R6 y el TAP simulando

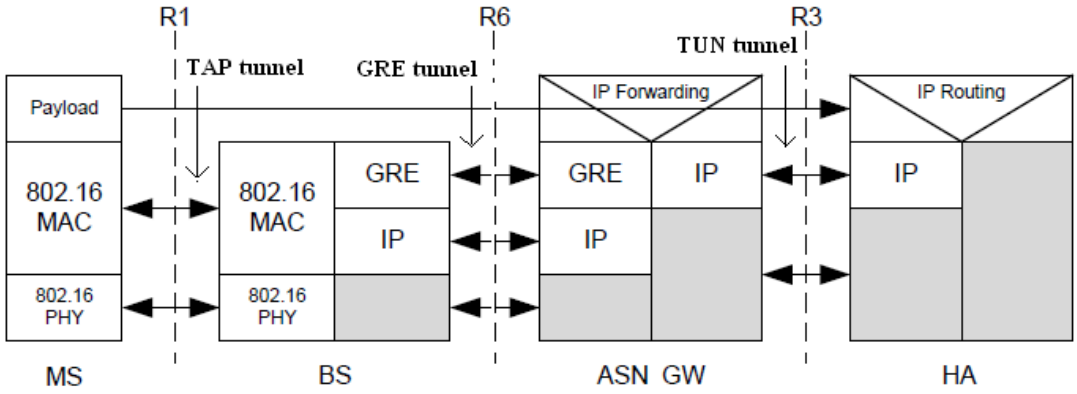


Figura 6 Torre de protocolos del plano de datos usados en boc-WiMAX

2.4.2 Escenario avanzado

Este escenario aumenta la complejidad respecto al escenario mostrado en el punto 2.4.1. Puesto que la misión principal de este despliegue será la validación del módulo de HO, necesitaremos contar al menos con una segunda BS. Decidimos también incorporar una segunda MS al despliegue, para validar el uso de la red por más de un usuario.

Haremos uso de las cuatro máquinas virtuales introducidas en el punto 2.4.1 y adicionalmente, sumaremos al despliegue otras dos máquinas más, boc-WiMAX_support1 y boc-WiMAX_support2. La primera realizará la función de BS y la segunda de MS.

Mostramos en la Figura 7 la configuración de red aplicada en este caso:

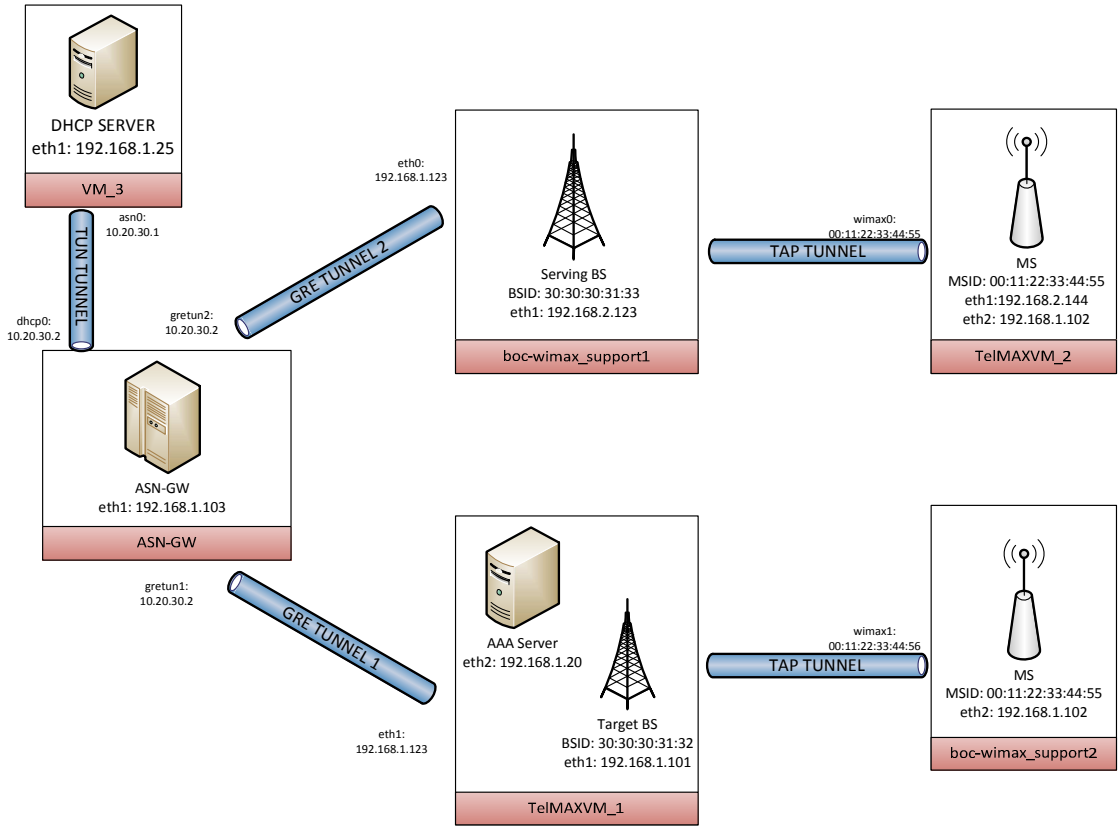


Figura 7 Esquema de red, escenario avanzado (tras el acceso a la red)

Es destacable resaltar que aparte de existir un MS y una BS más que en el escenario básico, también se ha añadido una segunda interfaz de red a la MS alojada en TelMAXVM_2, La funcionalidad de esta segunda interfaz está relacionada con el proceso de HO y será explicada con detenimiento en el apartado 5.3.

3 FUNCIONALIDADES CUBIERTAS EN boc-WiMAX

En este tercer capítulo detallaremos las funcionalidades que cubre la implementación *boc-WiMAX* de acuerdo al estándar 802.16e del IEEE (*Institute of Electrical and Electronics Engineers*) y las especificaciones de NWF.

La implementación *boc-WiMAX* puede obtenerse de forma gratuita como *software libre*. Como adelantamos en el capítulo 1º, esta implementación nos aporta el código en C++ de un ASN-GW, una estación base y una estación móvil WiMAX para ser ejecutadas en sistemas Linux y MacOS/X. No obstante, dicha implementación se encuentra inacabada y en la página de descarga [9] apenas encontramos información de los contenidos de dicha implementación, los requerimientos de compilación o una documentación precisa acerca de su alcance y su estado actual.

Por tanto, nuestra primera labor consistió en documentar e inspeccionar el código fuente de dicha implementación, detectar los errores y conseguir ejecutar el código de forma satisfactoria consiguiendo finalmente que el ASN-GW proporcione conectividad a nivel IP a la MS.

3.1 Compilación, configuración y ejecución de boc-WiMAX

Una vez obtenido el código de la implementación procederemos a compilarlo para obtener los ejecutables.

Para compilar la implementación deberemos contar con una IDE de C++. En nuestro caso usamos Eclipse.

Adicionalmente necesitaremos contar en el equipo donde deseemos compilar con las siguientes herramientas y librerias [9]:

- CMake (versión superior a la 2.6)
- glib
- GNUTLS
- libnet
- libpcap

Con este material instalado, nos bastará con ejecutar las siguientes sentencias dentro de la carpeta boc-WiMAX generada después de descargar la implementación:

```
mkdir build
cd build
cmake ..
make
```

Una vez compilado el proyecto obtendremos tres ejecutables distintos que resultarán alojados en el directorio boc-WiMAX/build/src. Dichos ejecutables serán boc-ms, boc-bs y boc-asn.

Antes de poder ejecutar la implementación debemos configurar el escenario en que queramos realizar las pruebas y comprobaciones. En este capítulo haremos uso del escenario básico descrito en el apartado 2.4.1. Este escenario, aparte de un ASN-GW y servidores DHCP y AAA, consta de una única estación base y una única estación móvil cuyas configuraciones serán explicadas mas adelante.

En primer lugar, deberemos establecer manualmente el túnel TUN entre la máquina virtual que aloja el ASN-GW y la máquina que aloja el servidor DHCP (ver Figura 7). Para ello, podemos elegir entre distintas alternativas como Open VPN o hacer uso de los dispositivos virtuales que ofrecen los sistemas Linux.

Los túneles GRE y TUN serán establecidos automáticamente por la implementación al ser ejecutada.

Debemos tener cada uno de los elementos de la red, ASN-GW, estación base, estación móvil, servidor DHCP y servidor AAA en cada una de las máquinas virtuales que corresponda siguiendo las directrices del escenario básico (apartado 2.4.1).

Finalmente deberemos configurar correctamente cada uno de los elementos. Cada uno de los ejecutables obtenidos dispone de un .conf asociado donde configurar ciertos parámetros. Adicionalmente deberemos configurar también el servidor AAA y el servidor DHCP para una correcta ejecución de la implementación.

- Configuración de la MS

Mostramos a continuación un ejemplo de configuración del archivo ms.conf

```
# Configuration file for the Mobile Station.

[ms]
interface=WiMAX0

[eap]
# If you want to use certificate validation (recommended) add:
#ca_cert=SomeCaCert.pem

# If you want to set the EAP outer identity to match the MSID add:
# anonymous_identity=%(msid)
identity=SomeUser
password=SomePassword
```

Con el campo *interface* podemos escoger el nombre del interfaz que sobre el cual se establecerá el túnel TUN en la MS.

En la parte [eap] podemos escoger el método de autenticación EAP a emplear por parte de la MS. Podemos escoger entre autenticar la MS mediante certificados o mediante una clave, aplicando en este último caso EAP-MD5. Finalmente también podemos emplear una identidad anónima que realizará el papel de usuario externo, en caso que deseemos emplear un túnel cifrado entre el servidor AAA y la MS.

Nota.- aunque el fichero de configuración indique la posibilidad de utilizar certificados, tras la verificación de la implementación, concluimos que el desarrollo actual de ésta sólo posibilita el empleo de autenticación basado en EAP-MD5.

- Configuración de la BS

Mostramos a continuación la configuración del archivo ms.conf para el despliegue inicial:

```
# Configuration file for the Base Station.

[asn]
port=2231
server=192.168.1.103

[bs]
id=30:30:30:30:31:32
server=192.168.1.101
broadcast=192.168.1.255
# port=32100
```

En la configuración referente al ASN-GW deberemos especificar de forma obligatoria de la IP en la que se encuentra el ASN-GW y el puerto UDP en el que se encuentra escuchando. Esta información es usada por la estación base para conectarse al ASN-GW y poder establecer el túnel GRE en la interfaz R6.

Seguidamente debemos configurar parámetros específicos de la estación base. Deberemos establecer su BSID, la IP que asignaremos a la BS y la dirección *broadcast* por la que comenzaremos a transmitir los mensajes DL-MAP. Estos mensajes son captados por las MSs y les otorgan la información básica de la BS para que puedan conectarse a ellas e iniciar el acceso a la red. Para mas información acerca de la utilidad de los mensajes DL-MAP, ver el apartado 3.3.3.1.

- Configuración del ASN-GW

Mostramos a continuación un ejemplo de configuración del archivo asn.conf

```
# Configuration file for the ASN GW.

[asn]
server=192.168.1.103
# port=2231
router=10.20.30.2

[dhcp]
server=10.20.30.1
tunnel=dhcp0

[radius]
server=192.168.1.20
secret=testing123
# port=1812
```

Tenemos tres partes diferenciadas de configuración; en la primera [asn], establecemos la IP donde se localizará el ASN-GW, el puerto de escucha y la dirección de router. Mediante esta última dirección se encaminará todo el tráfico desde el exterior a todas las MS gestionadas por el ASN-GW y viceversa.

En una segunda parte [dhcp], configuramos los parámetros necesarios para establecer el túnel TAP entre el ASN-GW y el HA (*Home Agent*) donde se encuentra el servidor DHCP.

Especificaremos la dirección IP donde se ubica dicho servidor DHCP y el nombre que le daremos al interfaz sobre el que quedará configurado el túnel en el extremo del ASN-GW.

Finalmente debemos configurar los parámetros para establecer la comunicación con el servidor Radius [radius]. La dirección IP donde se encuentra ubicado y la clave compartida (*secret*) entre el servidor Radius y el cliente Radius (el ASN-GW en nuestro caso). Esta clave puede contener hasta 127 caracteres alfanuméricos y va cifrada mediante el algoritmo MD5. También podemos establecer de forma opcional el puerto en el que escucha el servidor AAA. Por defecto usa el puerto UDP 1812.

- Configuración del Servidor DHCP dnsmasq

En el archivo dnsmasq.conf deberemos establecer simplemente dos campos:

```
interface=asn0
dhcp-range=10.20.30.10,10.20.30.199,255.255.255.0,1h
```

En el campo "interface", deberemos establecer el interfaz donde el servidor DHCP escuchara peticiones. Este interfaz deberá coincidir con el interfaz que hayamos asociado el extremo del túnel TAP.

También deberemos establecer el *pool* de direcciones que podrá usar el servidor DHCP para asignar a los clientes que le soliciten direcciones IP. En el ejemplo mostrado se especifica un rango de direcciones que van de la 10.20.30.10 a 10.20.30.199. También se especifica el tiempo que duración del préstamo de la IP. En nuestro caso se especifica una hora.

- Configuración del Servidor AAA freeradius

El servidor *freeradius* deberá ser configurado para atender las peticiones de los usuarios (MSs) a través de un cliente RADIUS (ASN-GW). Para ello nos dirigiremos a la carpeta donde tengamos ubicado el servidor y modificaremos los siguientes archivos:

a) clients.conf: En este archivo debemos establecer la clave compartida con el cliente y la dirección IP en la que se encuentra. Para ello introducimos las siguientes líneas:

```
client=192.168.1.103/24 {
        secret=testing123
}
```

b) users: En este archivo deberemos introducir las siguientes líneas:

```
00:11:22:33:44:55 Cleartext-Password := "jmgordillo"
        secret=testing123
        WiMAX-MSK +=%Introducir clave en hexadecimal de 512bits
```

En primer lugar introducimos la clave compartida asociada al identificador de usuario (MSID). Debemos recordar que como mecanismo de autenticación de la MS estamos usando EAP-MD5. Este mecanismo esta basado en el empleo de una clave compartida por el servidor y el cliente que va cifrada por el algoritmo MD5[10].

Adicionalmente para cada MS que queramos registrar en el servidor RADIUS, deberemos especificar los WiMAX RADIUS VSAs (*Vendor Specific Atributes*) que deseemos. Estos VSAs se encuentran definidos por el NWF en el stage 3 [5]. En esta configuración sólo definimos el VSA correspondiente a la MSK (*Master Session Key*). Esta clave resulta obligatoria para conseguir una correcta finalización del acceso a la red por parte de la MS. En capítulos posteriores se profundizará en las cuestiones relacionadas con la seguridad en WiMAX pero baste decir que a partir de esta clave se generará todo el material criptográfico empleado entre la BS y la MS.

Una vez configurados todos los agentes involucrados en el despliegue de la red, podemos pasar a ejecutarlos. Los servidores DHCP y Radius son ejecutados como demonios en sus respectivas máquinas virtuales.

/etc/init.d/dnsmasq start %sentencia de ejecución para el servidor dnsmasq

/etc/init.d/freeradius start %sentencia de ejecución para el servidor freeradius

Ahora tendremos que ejecutar respectivamente el ASN-GW, BS y MS en cada una de las máquinas virtuales donde los hayamos ubicados. Para ellos debemos introducir las siguientes sentencias dentro de las carpetas donde se hayan generado los ejecutables:

./boc-asn asn.conf %Ejecución del ASN-GW

./boc-bs bs.conf %Ejecución de la BS

./boc-ms –f ms.conf %Ejecución emulada. Trabaja con dispositivos emulados, comunicándose con la BS sobre IP.

3.2 Puesta a punto de la implementación boc-WiMAX

Para este punto, configuramos el despliegue de red básico descrito en el apartado 2.4.1. Una vez que tenemos el escenario configurado y todos los agentes en ejecución podemos pasar a depurar y corregir los errores que la implementación boc-WiMAX presenta en su versión gratuita.

Debemos recordar nuevamente que esta implementación se encuentra disponible al público en una versión inacabada, con errores de compatibilidad y prácticamente indocumentada.

Por ello, tendremos que realizar ciertas modificaciones sobre el código para poder poner en funcionamiento la implementación de forma satisfactoria.

Pasamos a continuación a detallar las modificaciones que tuvieron que ser realizadas sobre el código fuente de la implementación original para poder ser ejecutada con éxito:

1.- WiMAX_config *WiMAX_config_load(const char *config_file): Esta función, ubicada en el archivo config.c presenta como misión leer los parámetros de configuración del ASN-GW, BS o MS desde sus archivos de configuración. Esta función sólo contempla el carácter /n para localizar el final de cada línea y almacenar los valores. Este hecho resultó problemático, puesto que dependiendo de los sistemas operativos usados o de la distribución de un mismo *kernel* podemos encontrar que los finales de línea sean marcados con /n/r o solamente con /n.

El problema fue resuelto modificando el código de lectura de ficheros para hacerlo compatible con las distintas opciones de marcado de fin de línea que podamos encontrarnos en las distintas máquinas en que boc-WiMAX vaya a ser compilado.

2.- int WiMAX_interface_dhcp_start(const char *dev): Esta función, ubicada en el archivo interface.c, presenta como misión lanzar la ejecución del cliente DHCP ubicado en la MS. Una vez que el *network-entry* ha sido completado con éxito se debe solicitar una dirección IP al servidor DHCP. La implementación boc-WiMAX realiza esta petición realizando una llamada al sistema para ejecutar el cliente mediante la llamada **system** de C/C++.

Esta forma de ejecutar el cliente DHCP (udhcpc) también resultó problemática. Después de analizar la forma de funcionamiento de la implementación se llegó a la conclusión de que resultaba necesario reprogramar la función encargada de solicitar la ejecución del cliente DHCP aplicando concurrencia.

El funcionamiento original de la función WiMAX_interface_dhcp_start se muestra en la siguiente figura

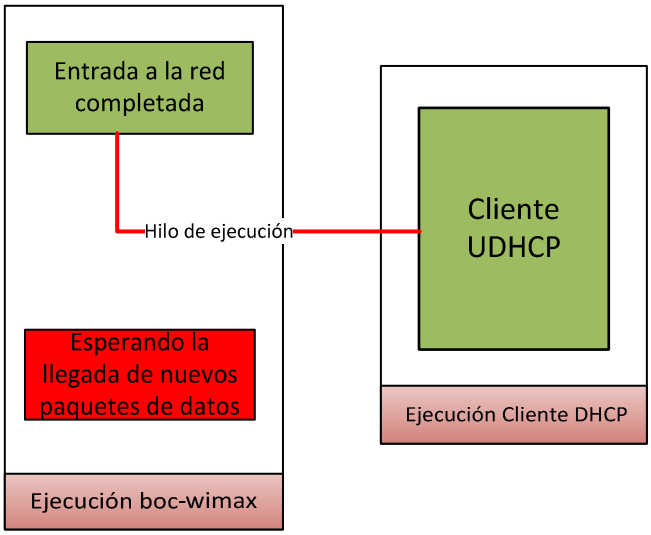


Figura 8 Línea de ejecución en boc-WiMAX

Podemos ver la problemática de realizar la llamada al cliente DHCP sin concurrencia. El proceso boc-ms pasará la línea de ejecución al cliente DHCP y quedará a la espera de que este termine su ejecución para volver a la actividad.

El cliente DHCP comenzará a enviar mensajes *Discovery* para solicitar una dirección IP al servidor DHCP. Este le responderá asignándole una dirección IP con el mensaje *offer*.

El problema surge en este punto, el mensaje *offer* debería ser recibido por la interfaz donde se encuentra escuchando la MS pero la línea de ejecución aún no ha sido devuelta al proceso boc-ms, con lo que no recibirá ningún mensaje por esa interfaz. Como consecuencia, el cliente DHCP no podrá finalizar nunca su ejecución y continuará enviando mensajes Discovery periódicamente.

En la Figura 9 mostramos la solución a este problema. Hacemos uso del concepto multi-hilo en programación concurrente. Vemos como la ejecución del proceso DHCP se realiza en una hebra distinta a la ejecución de boc-WiMAX. De esta forma la MS podrá adquirir una dirección IP y el proceso DHCP podrá finalizar.

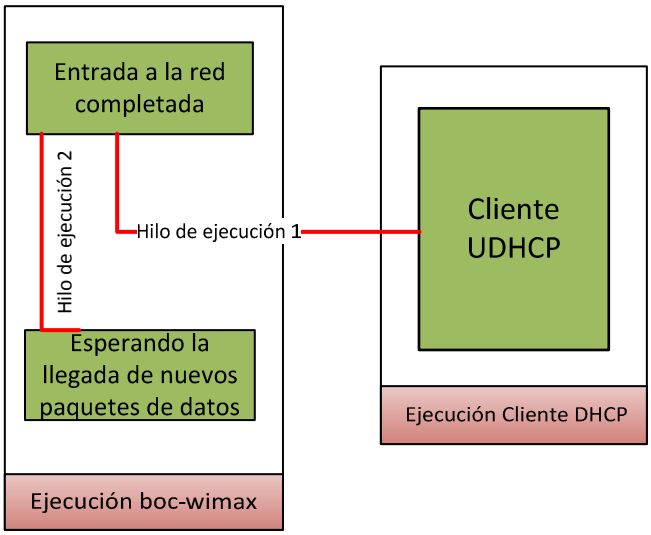


Figura 9 Línea de ejecución multi-hilo en boc-WiMAX

3.3 Funcionalidades originales de la implementación boc-WiMAX

La implementación boc-WiMAX, en su versión libre, cubre la fase de acceso de a la red descrita por el NWF[5] así como el procedimiento necesario para realizar la desconexión de la MS de la red de forma ordenada.

Se realizan los pasos descritos en la Figura 10 para poder conseguir finalmente conectividad a nivel IP.

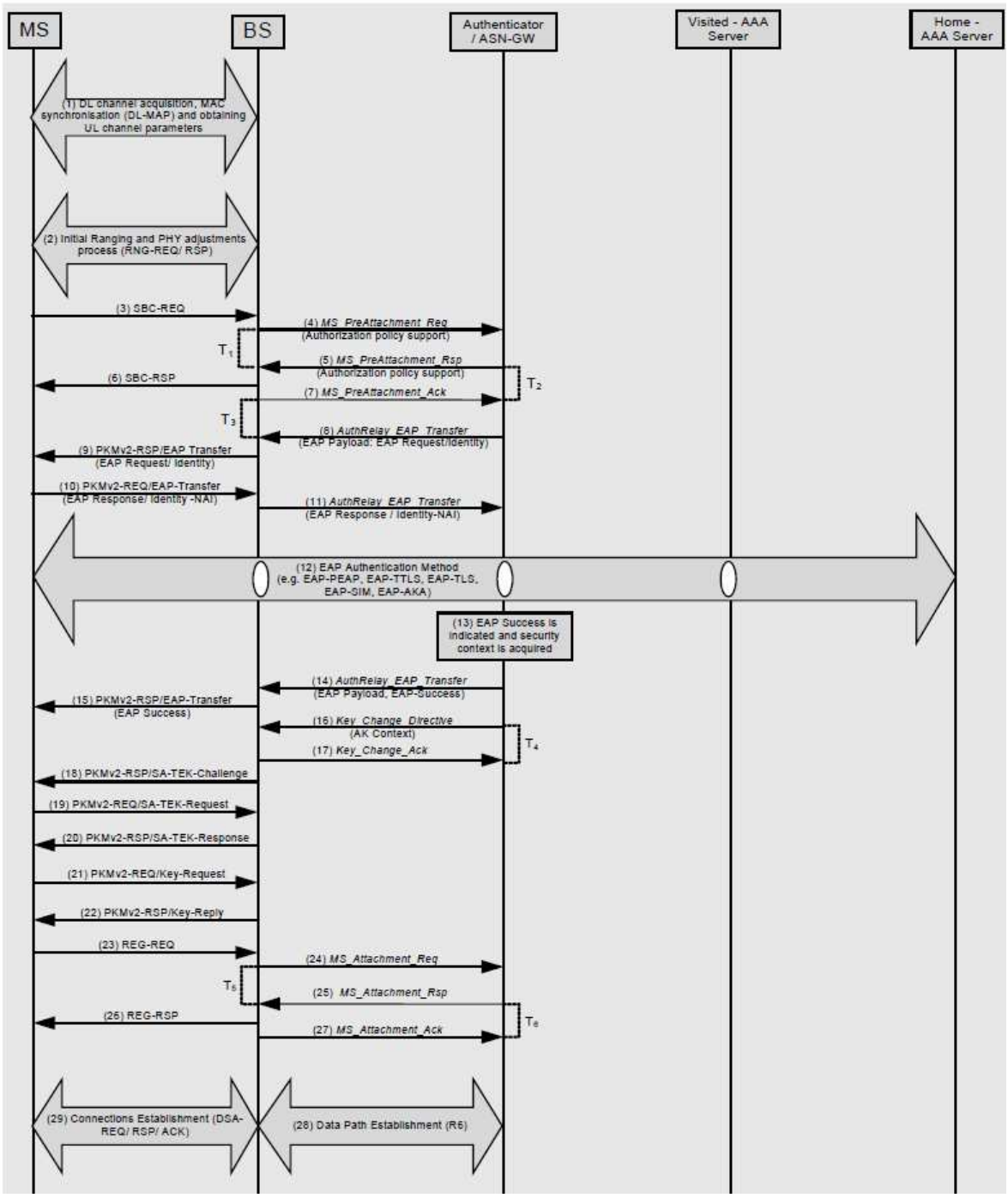


Figura 10 Etapas del acceso a la red

Antes de pasar a analizar el contenido de cada uno de los mensajes definidos en la Figura 10 debemos explicar el formato en el que se encuentran codificados.

3.3.1 Formato de mensajes de control en la interfaz R1

Este epígrafe explica el formato de los mensajes de control enviados entre la MS y la BS a través del interfaz radio (R1) empleado en la implementación boc-WiMAX. Debemos aclarar que la misión última de nuestro proyecto de fin de carrera es la elaboración una lógica de control que de soporte a los módulos de QoS y Handover en el ASN-GW y el interfaz R6. Por tanto tratamos de buscar una implementación que simplifique al máximo el interfaz R1 implementando las capacidades mínimas que nos permitan simular con un mínimo de realismo el intercambio de mensajes a través del canal radio.

boc-WiMAX nos ofrece un interfaz R1 simplificado. Como iremos viendo con posterioridad, la información y métodos propios del canal como modulaciones, RRM, frecuencias, etc. resultan obviados y no implementados.

Los mensajes se encuentran construidos de acuerdo con las directrices propuestas en el interfaz 802.16e del IEEE y se estructuran de la siguiente manera:

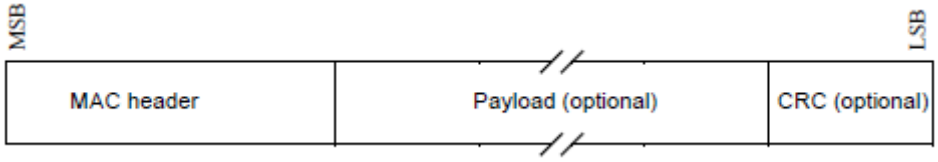


Figura 11 Formato MAC PDU

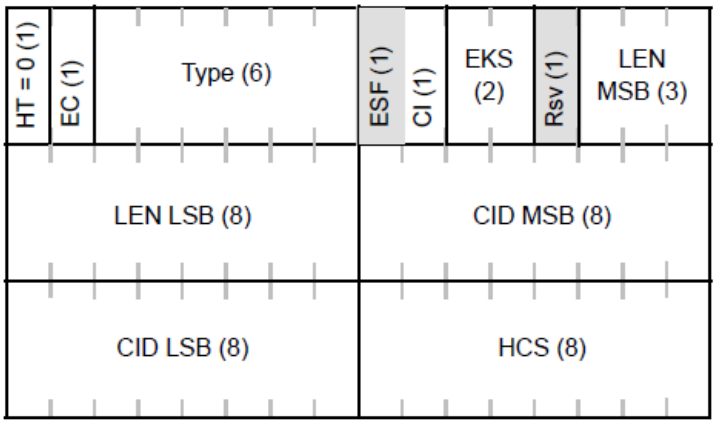


Figura 12 Formato cabecera MAC

boc-WiMAX codifica los campos descritos en la Figura 12 de la siguiente manera:

Tipo	Longitud (bits)	Codificación	Descripción
HT (Header Type)	1	0	valor asociado a la cabecera genérica
EC (Encryption control)	1	0	*payload* no encriptado o no incluido
Type	6	000000	ver Tabla 3

ESF (Extended Subheader Field)	1	0	*extended subheader* no incluida
CI (CRC indicator)	1	0	CRC no incluido
EKS (Encryption key sequence)	2	00	Índice de la clave TEK y vectores de inicialización usados en la encriptación del *payload*.
Rsv	1	0	-
LEN	11	variable	longitud en bytes del PDU incluyendo cabecera y CRC
CID (Connection Identifier)	16	variable	Identificador de flujo de tráfico a nivel MAC. Ver epígrafe 3.3.1.1
HCS (Header Check Sequence)	8	00000000	Detección de error en cabecera. No implementado en boc-WiMAX

Tabla 2 Codificación de los campos de la cabecera MAC en boc-WiMAX

Type bit	Value
#5 most significant bit (MSB)	*Reserved*
#4	ARQ feedback payload 1 = present, 0 = absent
#3	Extended type Indicates whether the present packing subheader (PSH) or fragmentation sub-header (FSH) is extended for non-ARQ-enabled connections 1 = Extended 0 = Not extended For ARQ-enabled connections, this bit shall be set to 1.
#2	Fragmentation subheader (FSH) 1 = present, 0 = absent
#1	Packing subheader (PSH) 1 = present, 0 = absent
#0 least significant bit (LSB)	DL: Fast-feedback allocation subheader (FFSH) UL: Grant management subheader (GMSH) 1 = present, 0 = absent

Tabla 3 Codificaciones del campo type de la cabecera MAC

Gracias al valor del CID sabremos distinguir si en el *payload* de la trama viaja información de gestión o datos.

Los mensajes de gestión van insertados en el campo *payload* descrito en la Figura 13. Siguen la siguiente estructura:

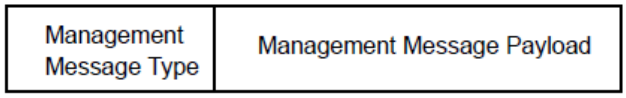


Figura 13 Formato de mensajes de gestión MAC

Cada tipo de mensaje presenta su propia estructura.

3.3.1.1 CID (Connection Identifier)

Entendemos por conexión como una conexión a nivel MAC entre la BS y la MS. Se establece un mapeo univoco entre la conexión a nivel MAC de la pareja MS-BS y el CID (ya sea en el canal de bajada o subida). Este CID a un SFID (*Service Flow Identifier*).

CID	Valor	Descripción
Initial	0x0000	Usado por BS y MS durante el proceso de ranging
Basic	0x0001-m	Mismo valor empleado para los canales DL y UL empleados en la conexión
Primary Managment	m+1-2m	Mismo valor empleado para los canales DL y UL empleados en la conexión
Transport, Secondary Managment	2m+1-0xFE9F	Mismo valor empleado para los canales DL y UL empleados en la conexión
Broadcast	0xFFFF	Usado para transmitir información en el canal de bajada (DL) a todas las MSs

Tabla 4 Tipos de CID empleados en boc-WiMAX

3.3.2 Formato de mensajes de control en el interfaz R6

Los mensajes de control enviados a través del interfaz R6, entre ASN-GW y BSs, se rigen mediante el ASN control protocol. Este protocolo se encuentra definido por el NWF[5].

Estos mensajes se envían mediante UDP. La cabecera del ASN control protocol comienza inmediatamente después de la cabecera del protocolo de transporte UDP. En la siguiente figura ilustramos la estructura de la cabecera.

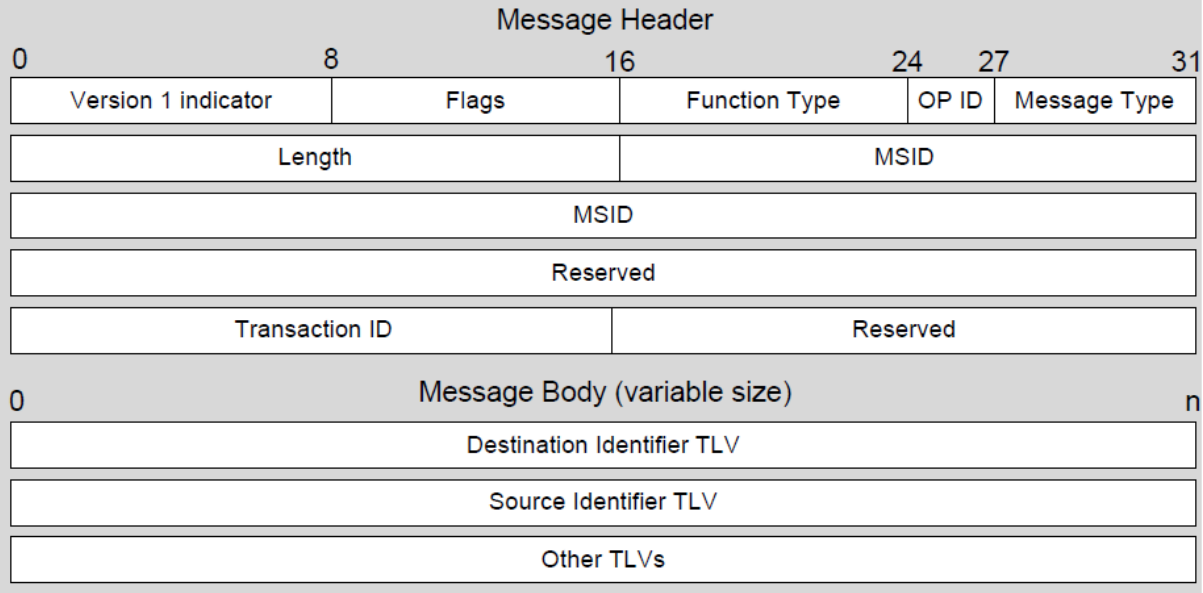


Figura 14 Formato de mensajes del ASN *control protocol*

boc-WiMAX codifica los campos descritos en la Figura 14 de la siguiente manera:

Tipo	Longitud (bits)	Codificación	Descripción
Version Indicator	8	00000001	Versión de protocolo empleada. Actualmente sólo la versión 1 se encuentra implementada
Flags	8	00000000	Ver epígrafe 3.3.2.1
Function Type	8	Variable	Tipo de función en la que se encuadra el mensaje.
OP ID	3	Variable	Indica el tipo de operación del mensaje. Ver epígrafe
Message Type	5	Variable	Tipo de mensaje dentro una función.
Length	16	Variable	Longitud del mensaje en bytes (incluyendo cabecera)
MSID	48	Variable	Dirección MAC de la MS
Reserved	32	Campo a 0	Para uso futuro
Transaction ID	16	Variable	Identificador de transacción. Usado para identificar paquetes pertenecientes al mismo 2-way o 3-way transaction
Reserved	16	00000000	Detección de error en cabecera. No implementado en boc-WiMAX
Message Body	Variable	Variable	Datos
Destination Identifier TLV	Variable	Variable	TLV con Información del destino
Source Identifier TLV	Variable	Variable	TLV con Información del origen

TLVs	Variable	Variable	Unidades de información establecidas de acuerdo a un formato estándar. Ver punto 3.3.2.3

Tabla 5 Codificación de los campos de la cabecera del protocolo ASN control

3.3.2.1 Campo Flags

Este campo tiene el siguiente significado:

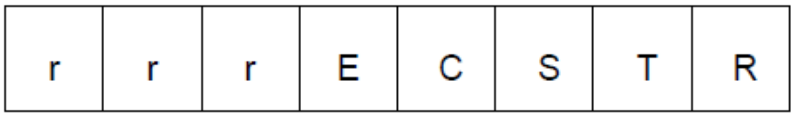


Figura 15 Campo Flags

- R: resetea el siguiente identificador Transaction ID esperado
- T: bit activo si el mensaje es enviado en modo de retransmisión. En este caso el ASN-GW no procesa el mensaje, simplemente procede a reenviarlo. Si este bit está activo los TLV Source y Destination Identifier son obligatorios.
- S: Usado para reconocer "*legacy nodes*" (nodos de red ajustados a una versión de esta especificación anterior a la 4)
- C: si este bit se encuentra activo, deshabilitamos la compresión de los campos Function Type, OP ID, Message Type. En boc-WiMAX el bit se encuentra inactivo.
- E: bit activo para indicar que se trata de una notificación de error del destino al origen del mensaje
- r: Bits reservados. Deben establecerse a 0.

Boc-WiMAX no realiza comprobación o procesado sobre el campo flag. Establece su valor como constante.

3.3.2.2 Campo OP-ID (Operation Identifier)

Este campo puede tener los siguientes significados:

Codificación	000	001	010	011	100	101/110/111
Significado	No permitido	Request/ Initiation	Response	Ack	Indication	Reservado

Tabla 6 Codificación del campo OP-ID

3.3.2.3 Formato TLV (Type Length Value)

El formato de estas unidades de información se muestra en la siguiente ilustración:

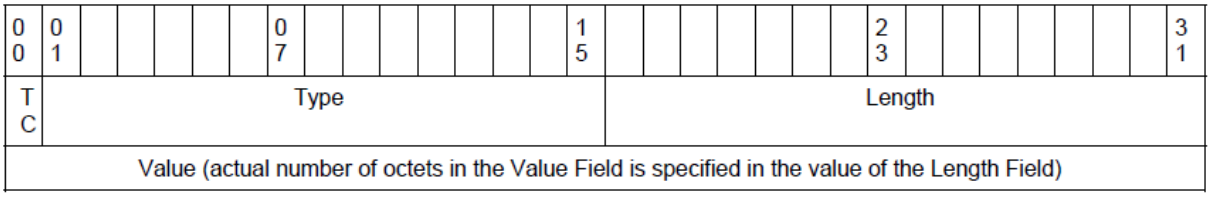


Figura 16 Formato TLV

- TC.- Si el bit vale 0, se debe procesar el TLV. Si el bit vale 1, la compresión del TLV no es requerida.
- Type.- Define el tipo de dato, ocupa 15 bits. Ej; type = 271 (TLV destination identifier)
- Length.- Define la longitud del campo *Value* en bytes.
- Value.- En este campo introducimos el valor asociado al TLV, ocupa 16 bits. También existe la posibilidad de anidar TLVs en este campo. Un TLV podría a su vez contener uno o varios sub-TLVs.

3.3.3 Fases del acceso a la red implementadas en boc-WiMAX

En este apartado vamos a describir la implementación que hace boc-WiMAX de cado uno de los pasos del acceso a la red descritos en la Figura 10.

Estos pasos pueden agruparse en seis bloques diferenciados. Son mostrados en la siguiente ilustración.

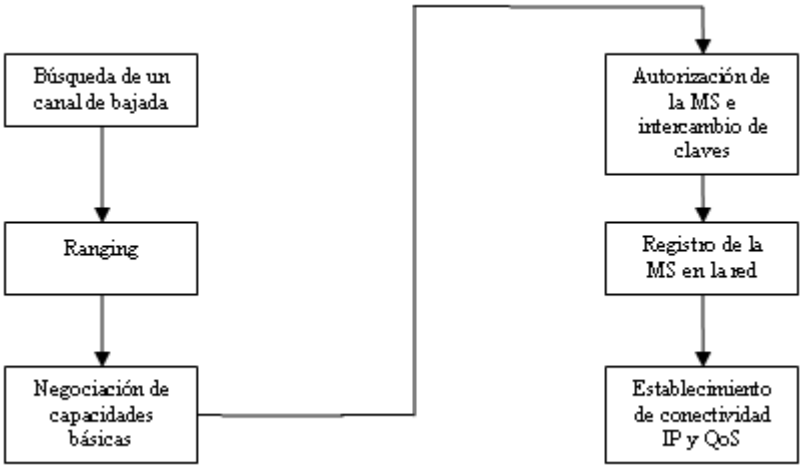


Figura 17 Fases del acceso a la red, implementadas en boc-WiMAX

Cada uno de estos bloques aglutina uno o varios de los mensajes enviados a través de los interfaces R1 y/o R6. A continuación se muestra el contenido de cada uno de los bloques. La numeración se corresponde con la establecida para cada uno de los pasos del acceso a la red, mostradas en la Figura 17.

- Búsqueda de un canal de bajada: (1)
- Ranging: (2)
- Negociación de capacidades básicas: (3), (4), (5), (6), (7)
- Autorización de MS e intercambio de claves: (8), (9) … (22)
- Registro de la MS en la red: (23), (24), (25), (26), (27)
- Establecimiento de conectividad IP y QoS: (28), (29)

3.3.3.1 Búsqueda de un canal de bajada

La BS, una vez iniciada, comienza a retransmitir periódicamente el mensaje DL-MAP a través del puerto 32100 de UDP (puerto por defecto, podemos cambiarlo en la configuración de la BS), estableciendo como destinatario la dirección de *broadcast* de la red en la que se encuentra la estación base (192.168.1.255). Por tanto, el envío del mensaje DL-MAP a través de la dirección de *broadcast* trata de simular lo que ocurriría en una situación real a través de la interfaz de radio. En dicha situación, la estación base radiaría en una frecuencia determinada el mensaje DL-MAP. Cualquier estación móvil que penetré en la celda de cobertura proporcionada por la estación base y deseara conectarse a dicha BS, debería realizar un barrido en frecuencia hasta encontrar una frecuencia en la que se estuviera transmitiendo un DL-MAP y sincronizarse con la BS.

Por ello la emisión del mensaje DL-MAP a través de la interfaz radio por parte de la BS se simula con el envío de dicho mensaje a través de la dirección *broadcast* de la red. La simulación de la captación de dicho mensaje en una frecuencia determinada por una MS, se realiza otorgándole a una de la interfaces de red de la MS una dirección IP perteneciente a la misma red que la IP de la BS, y poniendo en escucha dicha MS en el puerto UDP establecido para el intercambio de mensajes en la interfaz R1 (el 32100).

El formato del mensaje DL-MAP según el estándar 802.16e[11] debe seguir la siguiente estructura:

Syntax	Size (bit)	Notes
DL-MAP_Message_Format() {	—	—
Management Message Type = 2	8	—
PHY Synchronization Field	*variable*	See appropriate PHY specification.
DCD Count	8	—
Base Station ID	48	—
Begin PHY-specific section {	—	See applicable PHY subclause.
if (WirelessMAN-OFDMA) {	—	—
No. OFDMA symbols	8	For TDD, the number of OFDMA symbols in the DL subframe including all AAS/permutation zone and including the preamble. For FDD, see 8.4.4.2.2.
}	—	—
for (i = 1; i <= n; i++) {	—	For each DL-MAP element 1 to n.
DL-MAP_IE()	*variable*	See corresponding PHY specification.
}	—	—
}	—	—
if !(byte boundary) {	—	—
Padding Nibble	4	Padding to reach byte boundary.
}	—	—
}	—	—

Figura 18 Formato del mensaje DL-MAP

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Broadcast	Identificador de Conexión
	Management Message type	2	Identificador de mensaje de control
	Base Station ID	30:30:30:31:32	Dirección MAC de la estación base (BSID)
TLVs		-	-

Tabla 7 Composición del mensaje DL-MAP en boc-WiMAX

El resto de campos no son implementados ya que especifican parámetros de la interfaz radio y en nuestra simulación no resultarán necesarios.

Una vez recibido el DL-MAP en la MS, dicha estación conoce la BSID de la estación base. En nuestro caso será la dirección MAC de la BS.

De nuevo, en una situación real, la estación base una vez sincronizada con la estación móvil a través del DL-MAP, debería transmitir a la estación móvil el mensaje DCD (DL *channel descriptor*). En este mensaje se incluye toda la información referente al canal de bajada: reglas de ajuste de potencia, modulación a emplear, etc. En boc-WiMAX se prescinde del envío de este mensaje.

Cabe destacar que existen mensajes similares a los mensajes DCD y DL-MAP para definir las características del canal de subida (*uplink*). Estos mensajes son el UCD y el UL-MAP. No obstante, en

la implementación boc-WiMAX original, no se realiza ninguna distinción entre el canal de subida y bajada, por tanto, basta con la definición de uno de los dos canales ya que la configuración resultará idéntica para el otro canal.

3.3.3.2 Ranging

El inicio de esta fase se establece una vez que la MS queda sincronizada con la BS y los parámetros de los canales de subida y bajada han sido negociados. En una primera etapa, la MS envía un RNG-REQ (*ranging request*) a la BS. En este paso la estación móvil ya conoce la dirección MAC de la estación base, por ello, puede enviarle mensajes de gestión a través de la capa MAC, en boc-WiMAX se transmite vía Ethernet.

La función de esta solicitud consiste en estipular el retardo de la red y solicitar, como estación suscriptora, un perfil de transmisión para el canal y los niveles de potencia entre los que debe emitir.

Syntax	Size (bit)	Notes
RNG-REQ_Message_Format() {	—	—
Management Message Type = 4	8	—
Reserved	8	Shall be set to zero
TLV Encoded Information	*variable*	TLV-specific
}	—	—

Figura 19 Formato del mensaje Ranging-Request

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Initial	Identificador de Conexión
	Management Message type	4	Identificador de mensaje de control
TLV		**Tipo**	**Descripción**
SS MAC Address		00:11:22:33:44:55	MSID del suscriptor

Tabla 8 Composición del mensaje RNG-REQ en boc-WiMAX

Cuando el mensaje RNG-REQ es recibido en la BS, se procede a registrar la MS a través de su dirección MAC. Posteriormente se envía la respuesta (RNG-RSP) a la MS. El formato de dicho mensaje es idéntico al mostrado en la Figura 19 con la salvedad del valor que toma el campo Management Message Type, en esta ocasión será 5.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	5	Identificador de mensaje de control
TLV		**Tipo**	**Descripción**
Basic CID		Variable	Número de identificador de conexión básico. Ver apartado 3.3.1.1
Primary Management CID		Variable	Número de identificador de conexión primario. Ver apartado 3.3.1.1

Tabla 9 Composición del mensaje RNG-RSP en boc-WiMAX

3.3.3.3 Negociación de capacidades básicas

3.3.3.3.1 SBC-REQ

Una vez que la MS obtiene los identificadores de conexión básicos y primarios se procede a iniciar la negociación de las capacidades básicas. Esta negociación comienza con la transmisión del mensaje SBC-REQ (*SS Basic capabilitys request*) desde la MS a la BS. Mostramos el formato de dicho mensaje:

Syntax	Size (bit)	Notes
SBC-REQ_Message_Format() {	—	—
Management Message Type = 26	8	—
TLV Encoded Information	*variable*	TLV-specific
}	—	—

Figura 20 Formato del mensaje SBC-REQ

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	26	Identificador de mensaje de control
TLVs		-	-

Tabla 10 Composición del mensaje SBC-REQ en boc-WiMAX

En esta ocasión no se transmite ningún TLV. Nuevamente esta información está relacionada con el canal radio y la forma en la que debemos transmitir los datos a través de él, al simular este canal mediante una red Ethernet no es necesario incluirla. En una situación real deberíamos negociar capacidades referentes al ancho de banda, versión de protocolo PKM, política de autorización

soportada, tipos de moduladores y demoduladores empleados, parámetros específicos de la modulación OFDM, máxima potencia transmitida, etc.

Boc-WiMAX simplemente envía un mensaje de gestión de tipo SBC-REQ a la estación base pero no incluye información dentro de él.

3.3.3.3.2 MS_Preattachment-REQ

Una vez que el SBC-REQ es recibido en la estación base, esta envía un mensaje al ASN-GW notificando la entrada de una nueva estación móvil en la red.

Este mensaje se envía mediante el protocolo del plano de control definido por el WiMAX Forum para los interfaces R6, R8 y R7. La estructura seguida por los mensajes pertenecientes a este protocolo queda definida en la sección 3.3.2.

Boc-WiMAX codifica el mensaje MS_PreAttachment-Req de la siguiente forma:

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	9	MS State
	OP_ID	1	OP Request
	Message Type	1	Preattachment-Req
	Source Identifier	variable	MSID
TLV		**Tipo**	**Descripción**
MS Info		103	-
MS Info Sub-TLVs	**MSID**	variable	MSID
	Authorization Policy Support	0x11	Autenticación EAP
BS Info		26	-
BS Info Sub-TLVs	**BSID**	variable	BSID

Tabla 11 Composición del mensaje MS_Preattachment-Req en boc-WiMAX

Con este mensaje el ASN-GW es consciente de la solicitud de acceso a la red por parte de una MS. Adicionalmente se indica el método de autenticación que dicha MS soporta. El estándar 802.16e [11] establece dos tipos posibles de autenticación; basada en certificados vía RSA o mediante EAP. Boc-WiMAX solamente soporta autenticación EAP.

3.3.3.3.3 MS_Preattachment-RSP

Con este mensaje se consigue que la MS quede registrada en el ASN-GW. Se almacena su MSID y el BSID de la estación base a través de la cual se conecta a la red. Finalmente se aprueba la política de autorización solicitada en caso de ser soportada.

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	9	MS State
	OP_ID	2	OP Response
	Message Type	1	Preattachment-Rsp
	Source Identifier	variable	MSID
TLV		**Tipo**	**Descripción**
MS Info		103	-
MS Info Sub-TLVs	**MSID**	variable	MSID
	Authorization Policy Support	0x11	Autenticación EAP

Tabla 12 Composición del mensaje MS_Preattachment-Rsp en boc-WiMAX

3.3.3.3.4 SBC-RSP

Una vez que la BS recibe el mensaje MS_PreAttachment_Rsp procede enviar el SBC-RSP a la estación móvil y el MS_PreAttachment_Ack al ASN-GW. El formato del mensaje es igual al mostrado en la Figura 20 cambiando el tipo 26 por el 27.

En este mensaje se deberían confirmar las capacidades solicitadas por la estación móvil en el SBC-REQ cuando puedan ser soportadas, y adicionalmente se debería enviar todos los parámetros necesarios relativos a la transmisión de datos a través de la interfaz radio.

En boc-WiMAX simulamos este proceso enviando un mensaje a la MS con el código definido en el estándar para el mensaje SBC-RSP pero no se codifica ningún TLV dentro de él.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	27	Identificador de mensaje de control
TLVs		-	-

Tabla 13 Composición del mensaje SBC-RSP en boc-WiMAX

3.3.3.3.5 MS_Preattachment-ACK

Este mensaje confirma al ASN que la BS procedió en enviar el SBC-RSP a la estación móvil. Cabe destacar que con este *ack* no se confirma en ningún modo la correcta recepción del SBC-RSP por parte de la MS.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	9	MS State
	OP_ID	3	OP Ack
	Message Type	1	Preattachment-Ack
	Source Identifier	variable	MSID
TLVs		-	-

Tabla 14 Composición del mensaje MS_Preattachment-Ack en boc-WiMAX

3.3.3.4 Autorización MS e intercambio de claves

3.3.3.4.1 AuthRelay EAP-Identity Req Transfer

El autenticador (ASN-GW) inicia el procedimiento de autenticación con la MS vía EAP. El inicio de este proceso se produce una vez finalizado el proceso de *pre-attachment*.

El ASN-GW envía en primer lugar el EAP-Req a la BS a través de un mensaje tipo AR_EAP_Transfer solicitando a la MS su identidad.

El esquema de seguridad implementado en boc-WiMAX emplea el método EAP-MD5 [12] sobre RADIUS [13].

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	8	Authentication Relay
	OP_ID	1	OP Req
	Message Type	2	EAP transfer
	Source Identifier	variable	MSID
TLV		**Tipo**	**Descripción**
EAP Payload		62	EAP Indentity Request

Tabla 15 Composición del mensaje AR EAP Transfer / EAP-Indentity Req en boc-WiMAX

La explicación del método de autenticación EAP-MD5 se encuentra fuera del ámbito de estudio de este proyecto. No obstante, a grande rasgos podemos indicar que con este mensaje se inicia el mecanismo de autenticación de la MS haciendo uso del protocolo EAP. En esta primera fase de dicho protocolo se solicita la identidad de la MS que desea autenticarse en la red.

3.3.3.4.2 PKMv2-RSP / EAP-Identity ReqTransfer

La estación base retransmite hacia la estación móvil el EAP Request / Identity (recibido mediante el mensaje AR_EAP_Transfer) a través del mensaje PKMv2-RSP. La BS encapsula la información a retransmitir en el campo de datos de trama MAC haciendo uso del protocolo PKMv2.

Para aclarar la arquitectura de seguridad empleada en el interfaz R1 mostramos la siguiente figura:

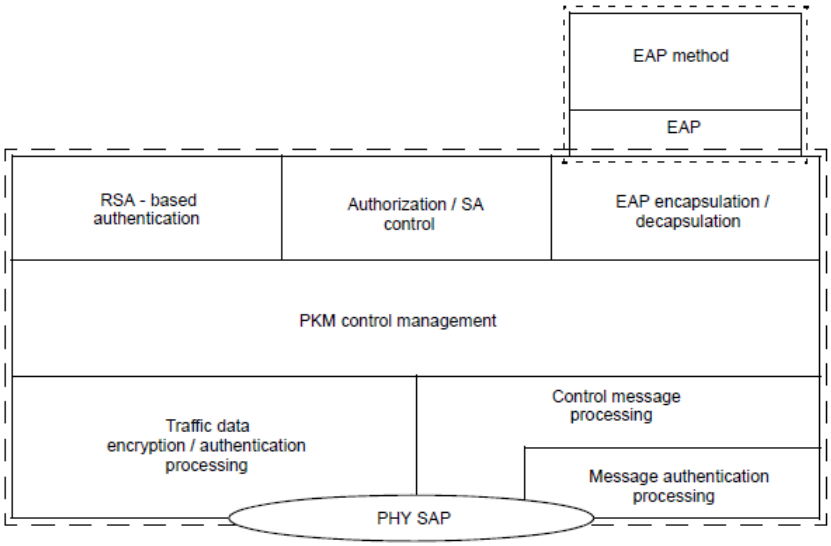


Figura 21 Capa de seguridad en el interfaz R1

En la Figura 21 observamos la torre de protocolos empleados en el estándar 802.16e en el nivel de seguridad.

En el nivel PKM podemos optar por emplear la versión 1 o 2 del protocolo. En boc-WiMAX se usa el protocolo PKMv2. En la capa superior se opta por autenticación basada en EAP y como método se especifica MD5.

A continuación mostramos la estructura y composición del mensaje.

Syntax	Size (bit)	Notes
PKM-RSP_Message_Format() {	—	—
Management Message Type = 10	8	—
Code	8	—
PKM Identifier	8	—
TLV Encoded Attributes	*variable*	TLV-specific
}	—	—

Figura 22 Formato del mensaje PKMv2-RSP

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	10	Identificador de mensaje de control
	Code	18	EAP Transfer
	PKM Identifier	1	EAP_PKM_identifier
TLV		**Tipo**	**Descripción**
PKM_EAP_Payload		28	EAP –Req [Identity]

Tabla 16 Composición del mensaje PKMv2 RSP / EAP Identity Req en boc-WiMAX

3.3.3.4.3 PKMv2-REQ / EAP-Identity RspTransfer

La MS responde al autenticador proporcionado su NAI (Network Access Identifier). Para ello encapsula la información de la capa EAP dentro del mensaje PKM-RSP.

Syntax	Size (bit)	Notes
PKM-REQ_Message_Format() {	—	—
Management Message Type = 9	8	—
Code	8	—
PKM Identifier	8	—
TLV Encoded Attributes	*variable*	TLV-specific
}	—	—

Figura 23 Formato del mensaje PKMv2-REQ

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	9	Identificador de mensaje de control
	Code	18	EAP Transfer
	PKM Identifier	variable	EAP_PKM_identifier
TLV		**Tipo**	**Descripción**
PKM_EAP_Payload		28	EAP –Req [Identity] NAI: MSID

Tabla 17 Composición del mensaje PKMv2 REQ / EAP Identity Rsp en boc-WiMAX

3.3.3.4.4 AuthRelay EAP-Identity Rsp Transfer

La BS obtiene el EAP *payload* transmitido en el mensaje definido en el punto 3.4.4.3 y lo reenvía al ASN-GW mediante el protocolo ASN *control protocol.*

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	8	Authentication Relay
	OP_ID	2	OP Rsp
	Message Type	2	EAP transfer
	Source Identifier	variable	MSID

TLV	Tipo	Descripción
EAP Payload	62	EAP –Rsp [Identity] NAI: MSID

Tabla 18 Composición del mensaje AR EAP Transfer / EAP-Identity Rsp en boc-WiMAX

3.3.3.4.5 Método de autenticación EAP

En este punto se ejecuta el método EAP escogido, en boc-WiMAX MD5. Una vez que el ASN-GW recibe el mensaje descrito en el apartado 3.4.4.4 procede a solicitar al servidor AAA la autenticación de la MS

En la Figura 24 mostramos el proceso completo de autenticación empleado en boc-WiMAX. El protocolo escogido para autenticar es EAP sobre Radius y el método, como citamos anteriormente, MD5.

Los mensajes (1) y (2) se corresponden con los mensajes descritos en los apartados 3.4.4.3 y 3.4.4.4

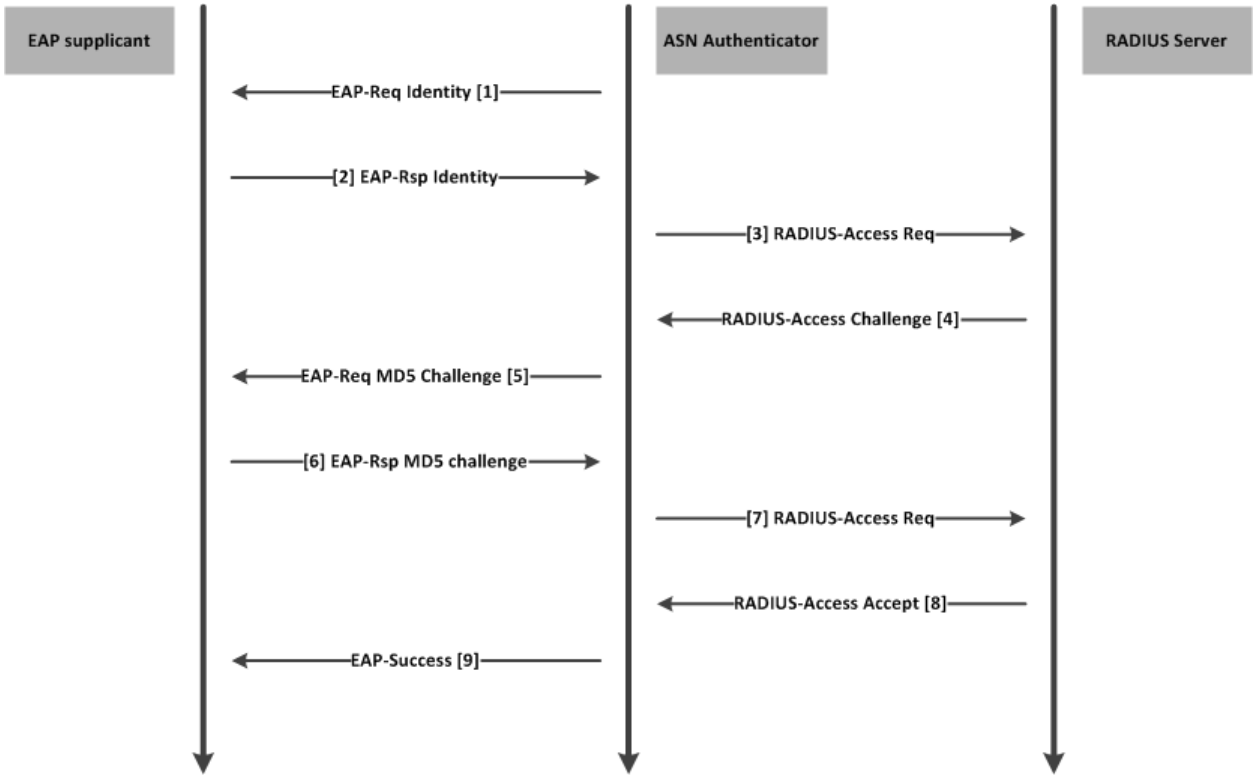


Figura 24 Fases de autenticación del método EAP empleado en boc-WiMAX

El EAP *supplicant* mostrado en la figura se encuentra alojado en la MS, el ASN *authenticator* se corresponde con el ASN-GW ya que sólo contemplamos el uso de un único ASN-GW en la arquitectura de red.

3.3.3.4.5.1 RADIUS-Access Req (3)

En el ASN Authenticator disponemos de un cliente RADIUS. Este cliente iniciará una fase de autenticación con el servidor RADIUS con la finalidad de autenticar a la MS.

Antes de continuar mostramos en la Figura 25 el esquema de un mensaje del protocolo RADIUS.

El campo *Code* identifica el tipo de mensaje RADIUS, el campo *Packet Identifier* tiene como objetivo validar las solicitudes y respuestas del proceso. El campo *Length* indica la longitud total del paquete RADIUS.

El campo *Authenticator* es usado para verificar mutuamente al servidor y cliente RADIUS empleando para ello un secreto compartido entre ellos.

Finalmente podemos encontrar una serie de AVPs (*Atribute Value Pairs*)

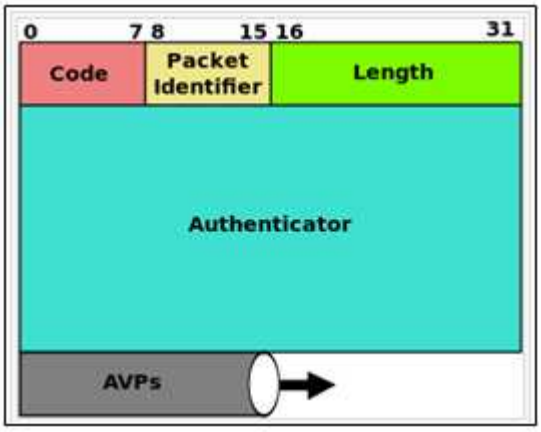


Figura 25 Estructura de un mensaje RADIUS

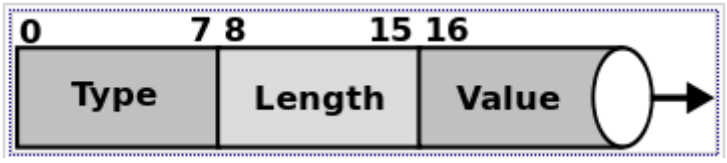


Figura 26 Estructura de un AVP

Estos campos son los encargados de transportar los datos necesarios para completar el proceso de autenticación.

AVPs	Valor	Descripción
NAS-IP Address	Variable	Dirección IP del cliente RADIUS
NAS-Port	0	Puerto de escucha del cliente RADIUS
Service-Type	8	Authenticate-Only
User-Name	NAI	Debe existir un registro de ese NAI en la base de datos del servidor RADIUS

EAP-Message	Variable	Response. Contiene el campo Identity = NAI
Message Authenticator	Variable	HMAC-MD5 hash obtenido a partir del mensaje RADIUS completo y el secreto compartido entre el cliente y el servidor RADIUS.

Tabla 19 AVPs codificados en el mensaje RADIUS Access-Request

3.3.3.4.5.2 RADIUS-Access Challenge (4)

El servidor RADIUS envía este mensaje solicitando una respuesta al cliente. Incrementa la seguridad del proceso al solicitar información adicional al cliente. Adicionalmente sobre RADIUS se enviará también el EAP-challenge elaborado mediante la clave compartida entre la MS y el servidor RADIUS empleando el cifrado MD5. Este challenge se utiliza según el protocolo CHAP [Challenge-Handshake Authentication Protocol] para autenticar a la MS mediante la técnica de desafío mutuo.

AVPs		Valor	Descripción
Vendor-Specific	**MSK**	Variable	Clave de sesión maestra a partir de cual empezaremos a generar el material criptográfico necesario a emplear en el interfaz radio. Enviada después de una autenticación EAP exitosa
Message Authenticator		Variable	HMAC-MD5 hash obtenido a partir del mensaje RADIUS completo y el secreto compartido entre el cliente y el servidor RADIUS.
EAP-Message		Variable	Request. Contiene el EAP-Challenge obtenido mediante cifrado MD5 en base al password compartido por el cliente EAP y el servidor Radius
State		Variable	Debe ser enviado de vuelta al servidor de forma inalterada

Tabla 20 AVPs codificados en el mensaje RADIUS Access-Challenge

3.3.3.4.5.3 AuthRelay / EAP-Request MD5 Challenge (5)

Una vez que el ASN-GW recibe el mensaje RADIUS-Access Challenge procede a reenviar la información asociada al protocolo EAP incluida en dicho mensaje a través del interfaz R6. Para el reenvío se utiliza el ASN *control protocol*.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	8	Authentication Relay

	OP_ID	1	OP Req
	Message Type	2	EAP transfer
	Source Identifier	variable	MSID
TLV		**Tipo**	**Descripción**
EAP Payload		62	EAP –MD5 Challenge

Tabla 21 Composición del mensaje AR EAP Transfer / EAP-Req MD5 Challenge

3.3.3.4.5.4 PKMv2-RSP / EAP-Transfer (5)

La BS procede a reenviar el EAP-MD5 Challenge a la MS mediante el protocolo 802.16e [11]

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	10	Identificador de mensaje de control
	Code	18	EAP Transfer
	PKM Identifier	variable	EAP_PKM_identifier
TLV		**Tipo**	**Descripción**
PKM_EAP_Payload		28	EAP –Rsp [MD5 Challenge]

Tabla 22 Composición del mensaje PKMv2 RSP / ChallengeMD5 Rsp

3.3.3.4.5.5 PKMv2-REQ / EAP-Transfer (6)

El reto llega al cliente EAP. Este aplica el secreto compartido y el algoritmo MD5 para realizar una función de hash sobre el reto recibido y lo manda de vuelta al servidor RADIUS.

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	9	Identificador de mensaje de control
	Code	18	EAP Transfer
	PKM Identifier	variable	EAP_PKM_identifier
TLV		**Tipo**	**Descripción**
PKM_EAP_Payload		28	EAP –Req [hash(MD5 Challenge)]

Tabla 23 Composición del mensaje PKMv2 REQ / ChallengeMD5 Req en boc-WiMAX

3.3.3.4.5.6 AuthRelay / EAP-Response MD5 Challenge (6)

La BS reenvía el EAP payload recibido en el mensaje descrito en el punto 3.4.4.5.5 al ASN-GW

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	8	Authentication Relay
	OP_ID	2	OP Rsp
	Message Type	2	EAP transfer
	Source Identifier	variable	MSID
TLV		**Tipo**	**Descripción**
EAP Payload		62	EAP –hash[MD5 Challenge]

Tabla 24 Composición del mensaje AR EAP Transfer / EAP-Rsp MD5 Challenge

3.3.3.4.5.7 RADIUS-Access Req(7)

AVPs	Valor	Descripción
NAS-IP Address	variable	Dirección IP del cliente RADIUS
NAS-Port	0	Puerto de escucha del cliente RADIUS
Service-Type	8	Authenticate-Only
User-Name	NAI	Debe existir un registro de ese NAI en la base de datos del servidor RADIUS
EAP-Message	variable	Response. Contiene el campo MD5-Challenge
Message Authenticator	variable	HMAC-MD5 hash obtenido a partir del mensaje RADIUS completo y el secreto compartido entre el cliente y el servidor RADIUS.

Tabla 25 AVPs codificados en el mensaje RADIUS Access-Request

El cliente RADIUS responde a la petición de información adicional realizada por el servidor RADIUS mediante el mensaje RADIUS Access Challenge enviándole adicionalmente el EAP MD5 Challenge Rsp en el AVP EAP.

3.3.3.4.5.8 RADIUS-Access Accept (8)

El servidor RADIUS verifica la información recibida con su base de datos y si es correcto finalmente el cliente RADIUS queda autenticado. En paralelo, en el servidor AAA también se ubica el autenticador EAP, este verifica el EAP-MD5 Challenge Rsp de acuerdo al protocolo CHAP. Si la verificación resulta exitosa la MS queda autenticada y se procede a enviar el EAP success.

AVPs	Valor	Descripción
User-Name	NAI	Debe existir un registro de ese NAI en la base de datos del servidor RADIUS
EAP-Message	variable	EAP-Success
Message Authenticator	variable	HMAC-MD5 hash obtenido a partir del mensaje RADIUS completo y el secreto compartido entre el cliente y el servidor RADIUS.

Tabla 26 AVPs codificados en el mensaje RADIUS Access-Accept

La recepción de este mensaje por parte del ASN-GW desencadenará el envío de los mensajes descritos en los apartados 3.4.4.6 y 3.4.4.8 respectivamente.

3.3.3.4.6 Auth Relay / EAP-Success (9)

El ASN-GW reenvía el EAP success a la BS mediante el ASN control protocol.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	8	Authentication Relay
	OP_ID	1	OP Req
	Message Type	2	EAP transfer
	Source Identifier	variable	MSID
TLV		**Tipo**	**Descripción**
EAP Payload		62	EAP –Success

Tabla 27 Composición del mensaje AR EAP Transfer / EAP-Success en boc-WiMAX

Mostramos finalmente una captura de tráfico realizada en el ASN-GW. En ella hemos encuadrado en rojo los mensajes pertenecientes a al autenticación basada en el método EAP

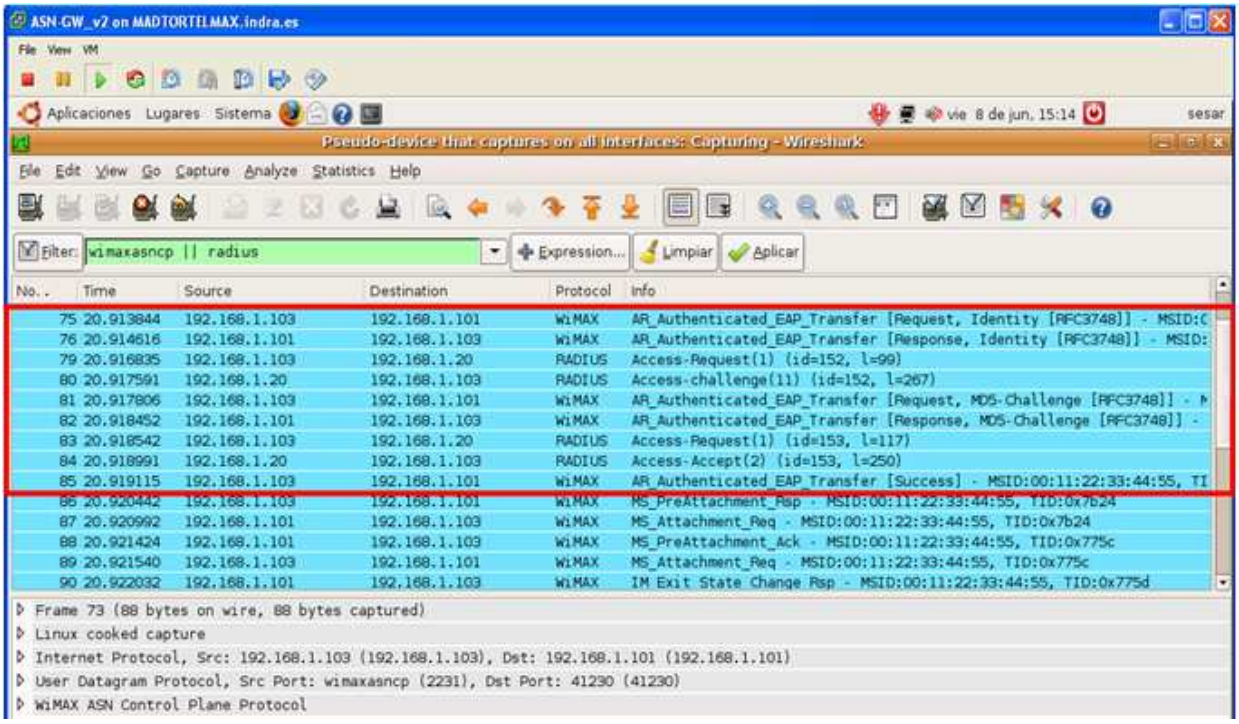


Figura 27 Captura de tráfico en el ASN-GW [proceso de autenticación EAP]

3.3.3.4.7 PKMv2-RSP / EAP Success

LA BS procede a reenviar a la MS el mensaje EAP-Success mediante el protocolo PKMv2.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	10	Identificador de mensaje de control
	Code	18	EAP Transfer
	PKM Identifier	variable	EAP_PKM_identifier
TLV		**Tipo**	**Descripción**
PKM_EAP_Payload		28	EAP –Success

Tabla 28 Composición del mensaje PKMv2 RSP / EAP Success en boc-WiMAX

3.3.3.4.8 Key Change Directive

El ASN-GW una vez recibido el mensaje Access-Accept por parte del servidor RADIUS procede a generar la clave AK (Authorization Key).

Esta clave se genera de acuerdo a las directrices establecidas en el estándar 802.16e[11].

La clave AK se deriva a partir de la MSK obtenida mediante el mensaje RADIUS-Accept Challenge descrito en el apartado 3.3.3.4.5.2.

La MSK es un clave de 512 bits que deben conocer el servidor AAA y la MS, a partir de ella generará el la clave AK.

En primer lugar se genera la clave PMK (Pairwise Master Key) truncando la MSK a 160 bits.

A continuación se aplica el algoritmo Dot16KDF introduciendo como entradas dicho algoritmo la PMK, MSID, BSID.

Como resultado obtenemos la clave AK con una longitud de 160 bits.

Una vez generada la clave AK debemos generar su contexto asociado y enviarlo a la BS que está dando servicio a la MS que desea acceder a la red. El contexto AK empleado en la autenticación EAP está formado por:

- AK: clave de 160 bits generada a partir de la clave PMK
- AK-ID: Identificador de clave. Longitud de 64 bits. Generada mediante el algoritmo Dot16KDF a partir de la clave AK, MSID, BSID y AK-SN
- AK-SN(Sequence Number): Número de secuencia de la clave AK. Presenta cuatro bits de longitud. Los dos bits menos significativos son el contador. Los dos bits más significativos se ponen a cero.
- AK-Lifetime: Tiempo durante el cual será válida la clave AK
- HMAC/CMAC_KEY_U: Clave usada para firmar los mensajes de control del canal de subida. Generada a partir de la clave AK

A continuación se muestra la composición del mensaje enviado por el ASN-GW a la BS.

Parámetro			**Valor**	**Descripción**
Parámetros de Cabecera		**Version**	1	Versión empleada del ASN control protocol
		Function Type	9	MS State
		OP_ID	1	OP Req
		Message Type	7	Key Change Directive
		Source Identifier	variable	MSID
TLV			**Tipo**	**Descripción**
BS Info			26	-
BS Info-Sub-	**AK-Context**	**AK**	variable	Clave 160 bits
		AK-ID	variable	Identificador de clave 60 bits
		AK-SN	variable	Número de secuencia de clave 4

TLVs				bits
		AK-lifetime	X	Campo no funcional en boc-WiMAX
		HMAC/CMAC_KEY_U	X	Campo no funcional en boc-WiMAX
Authorization Complete			17	-
Authorization Complete-Sub TLVs		**Authentication Result**	18	(0) Success
		PKM2 Message code	134	(18) EAP transfer

Tabla 29 Composición del mensaje MS State / Key change directive en boc-WiMAX

Cuando la BS recibe este procede a enviar el mensaje Key Change ACK al ASN-GW y el mensaje SA-TEK Challenge a la MS.

3.3.3.4.9 Key Change ACK

La BS confirma al ASN-GW que el contexto AK fue recibido con éxito.

La estructura del mensaje es idéntica a la mostrada en la Tabla 14.

3.3.3.4.10 PKMv2 RSP / SA-TEK-Challenge

La estación base envía este mensaje a través del protocolo PKMv2. Supone el inicio de la fase 3-way SA-TEK handshake formada por los mensajes 3.3.3.4.10, 3.3.3.4.11 y 3.3.3.4.12.

Con este mensaje se identifica la clave AK que debe ser usada. Adicionalmente se incluye un número aleatorio que hará la función de *challenge*, el cual deberá ser retornado a la BS en el mensaje PKMv2 SA-TEK Request.

El formato del mensaje descrito en el estándar 802.16e debe contener los siguientes campos:

Attribute	Contents
BS_Random	A freshly generated random number of 64 bits.
Key Sequence Number	AK sequence number.
AKID	Identifies the authorization key (this is the AKID of the *new* AK in the case of reauthentication).
Key lifetime	PMK lifetime, this attribute shall include only follows EAP-based authorization or EAP-based reauthorization procedures.
HMAC/CMAC Digest	Message authentication digest for this message.

Figura 28 Formato del mensaje PKMv2 RSP / SA-TEK Challenge

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	10	Identificador de mensaje de control
	Code	20	SA TEK Challenge
	PKM Identifier	Variable	EAP_PKM_identifier
TLV		**Tipo**	**Descripción**
PKM AKID		45	Identificador de clave AK
PKM Key Lifetime		9	Tiempo de vida de la clave AK
PKM Key Sequence Number		10	Número de secuencia de la clave AK

Tabla 30 Composición del mensaje PKMv2 RSP / SA-TEK Challenge en boc-WiMAX

Analizando los campos introducidos en la Tabla 30, podemos comprobar como boc-WiMAX no incorpora el *challenge* ni el HMAC/CMAC Digest. Este campo debería servir a la BS y MS para autenticar el mensaje.

El HMAC/CMAC digest se debería generar mediante funciones de hash realizadas sobre el mensaje partir de la clave HMAC/CMAC perteneciente al AK context descrito en el punto 3.3.3.4.8.

Por tanto, a pesar de realizar la autenticación de la MS mediante EAP MD5 y obtener el material criptográfico básico, no queda implementada la funcionalidad de autenticación de los mensajes de gestión en el interfaz R1 al no generarse las claves HMAC/CMAC.

3.3.3.4.11 PKMv2 REQ / SA-TEK Request

La estación móvil debería enviar este mensaje una vez verificado el HMAC/CMAC digest mediante la clave HMAC/CMAC generada a partir de la clave AK. En él deben incluirse los métodos criptográficos que desean emplearse para cifrar y autenticar los mensajes de datos, Ej.; DES 56 bits, AES 128 bits, etc.

Este mensaje debería contener los siguientes campos

Attribute	Contents
MS_Random	A 64-bit number chosen by the MS freshly for every new handshake[a]
BS_Random	The 64-bit random number used in the PKMv2 SA-TEK-Challenge message
Key Sequence Number	AK sequence number
AKID	Identifies the authorization key that was used for protecting this message
Security-Capabilities	The requesting MS's supported cryptographic suites (11.9.13)
Security Negotiation Parameters	The requesting MS's security capabilities (see 11.8.4)
HMAC/CMAC Digest	Message authentication digest for this message

Figura 29 Formato del mensaje PKMv2 REQ / SA-TEK Request

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	9	Identificador de mensaje de control
	Code	21	SA TEK Request
	PKM Identifier	Variable	EAP_PKM_identifier
TLV		**-**	**-**

Tabla 31 Composición del mensaje PKMv2 REQ / SA-TEK Request en boc-WiMAX

En boc-WiMAX este mensaje no implementa ningún TLV. No se contempla la negociación de ninguna *suite* criptográfica ni se realiza autenticación del mensaje mediante HMAC/CMAC.

Como vemos los mecanismos de seguridad necesarios para conseguir una comunicación confidencial entre la MS y la BS no quedan implementados en boc-WiMAX.

3.3.3.4.12 PKMv2 RSP / TEK Response

La BS finalmente envía este mensaje a la MS acabando así el 3-way SA-TEK handshake. Con este mensaje debería quedar definido el método criptográfico a emplear en la comunicación de datos entre BS y MS y definida la asociación de seguridad (SA) de la MS. Esta asociación es un conjunto de datos que definen completamente los métodos y materiales criptográficos que han de usarse en el canal de comunicación establecido entre la BS y la MS.

Boc-WiMAX no contempla la creación de SAs y por tanto implementa un canal de comunicación no seguro. Este hecho no resulta de vital importancia ya que como comentamos con anterioridad el canal radio trata de emularse y simplificarse al mínimo en la implementación.

Attribute	Contents
MS_Random	The number received from the MS.
BS_Random	The random number included in the PKMv2 SA-TEK-Challenge message.
Key Sequence Number	AK sequence number.
AKID	Identifies the authorization key to the MS that was used for protecting this message.
SA_TEK_Update	A compound TLV list each of which specifies a SAID and additional properties of the SA that the MS is authorized to access. This compound field may be present at the reentry only. For each active SA in previous serving BS, corresponding TEK, GTEK, and GKEK parameters are included.
Frame Number	An absolute frame number in which the old PMK and all its associate AKs should be discarded.
(one or more) SA-Descriptor(s)	Each compound SA-Descriptor attribute specifies a SAID and additional properties of the SA. This attribute is present at the initial network entry or reentry after receipt of a RNG-RSP message with HO Process Optimization bits (Bit 1, Bit 2)=(0,0).
Security Negotiation Parameters	The responding BS's security capabilities (see 11.8.4).
HMAC/CMAC Digest	Message authentication digest for this message.
PKM configuration settings	PKM configuration defined in 11.9.18

Figura 30 Formato del mensaje PKMv2 RSP / SA-TEK Response

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	10	Identificador de mensaje de control
	Code	22	SA TEK Response
	PKM Identifier	Variable	EAP_PKM_identifier
TLV		**-**	**-**

Tabla 32 Composición del mensaje PKMv2 RSP / SA-TEK Response en boc-WiMAX

3.3.3.4.13 PKMv2 REQ / Key Request

La MS debería enviar este mensaje solicitando una nueva TEK (Traffic Encryption Key) y sus parámetros asociados. Con esta clave estaríamos en condiciones de cifrar las transmisiones de datos que puedan realizarse en un futuro a través del canal radio.

Attribute	Contents
Key Sequence Number	AK sequence number
SAID	Security association identifier —GSAID for MBS
Nonce	A random number generated in an MS
HMAC/CMAC Digest	Message digest calculated using AK

Figura 31 Formato del mensaje PKMv2 REQ / Key Request

Nuevamente este mensaje no es funcional en la implementación boc-WiMAX.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	9	Identificador de mensaje de control
	Code	23	Key Request
	PKM Identifier	Variable	EAP_PKM_identifier
TLV		**-**	**-**

Tabla 33 Composición del mensaje PKMv2 REQ / Key request en boc-WiMAX

3.3.3.4.14 PKMv2 Key RSP / Key Reply

Con este mensaje la BS le otorga finalmente la clave TEK y los parámetros asociados a la MS.

Mensaje no funcional en boc-WiMAX.

Attribute	Contents
Key-Sequence-Number	AK sequence number.
SAID	Security Association ID.
TEK-Parameters	"Older" generation of key parameters relevant to SAID.
TEK-Parameters	"Newer" generation of key parameters relevant to SAID.
HMAC-Digest	Keyed SHA message digest.

Figura 32 Formato del mensaje PKMv2 RSP / Key reply

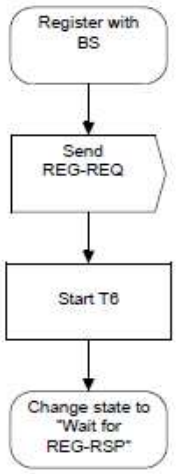
Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	10	Identificador de mensaje de control
	Code	24	Key Reply
	PKM Identifier	Variable	EAP_PKM_identifier
TLV		**-**	**-**

Tabla 34 Composición del mensaje PKMv2 RSP / Key reply en boc-WiMAX

3.3.3.5 Registro de la MS en la red

Una vez que los procedimientos de autenticación e intercambio de material criptográfico finalizan de forma satisfactoria, la MS queda autenticada y procede a registrarse en la estación base de acuerdo a la metodología propuesta en el estándar 802.16e [11].

Los pasos seguidos durante esta etapa se muestran de forma gráfica en la figura:



Como hemos mencionado con anterioridad, llegados a este punto, la MS ha quedado registrada y dicha estación envía el mensaje REG-REQ para solicitar que la BS retransmita el tráfico con origen en la MS a la red y viceversa.

Cabe destacar que en la implementación boc-WiMAX, el temporizador T6 no resulta implementado. Una vez que el mensaje REG-REQ es recibido en la BS, se espera a recibir el MS_Attachment_RSP (3.3.3.5.3) por parte del ASN-GW para enviar el REG-RSP a la MS sin establecer límite temporal alguno.

3.3.3.5.1 REG Request

Con este mensaje la MS solicita el registro en la red. En el pueden codificarse múltiples TLVs en el que se solicitan y acuerdan distintos parámetros para establecer la conexión. Algunos ejemplos de estos TLVs serían el máximo número de datos por trama en la capa MAC, soporte ARQ, parámetros para HO, ahorro de energía activo, etc.

En boc-WiMAX este mensaje resulta simplificado al mínimo, al igual que sucede con la gran mayoría de los mensajes del interfaz R1. Solamente queda indicada la versión del protocolo IP que deseamos usar.

Syntax	Size (bit)	Notes
REG-REQ_Message_Format() {	—	—
Management Message Type = 6	8	—
TLV Encoded Information	*variable*	TLV-specific
}	—	—

Figura 33 Formato del mensaje REG-REQ

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	6	Identificador de mensaje de control
TLV		**Tipo**	**Descripción**
IP Version		4	En boc-WiMAX se emplea IPv4

Tabla 35 Composición del mensaje REG-REQ

Como vemos en la implementación se usa IPv4.

AeroMACS en sus especificaciones establece que deberá soportar tanto IPv4 como IPv6, no obstante los prototipos de los elementos que conformarán futuro datalink en una primera fase deben funcionar sólo con IPv4, por lo que se decidió no adaptar el simulador boc-WiMAX a IPv6 en primera instancia.

3.3.3.5.2 MS Attachment Request

La BS después de recibir el REG-REQ envía el Attachment Request para informar al ASN-GW que la MS está solicitando ser registrada en la red

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	9	MS State
	OP_ID	1	OP Request
	Message Type	4	Attachment-Req
	Source Identifier	Variable	MSID
TLV		**Tipo**	**Descripción**
MS Info		103	-

MS Info Sub-TLVs	**MSID**	Variable	MSID

Tabla 36 Composición del mensaje MS Attachment Request

3.3.3.5.3 MS Attachment Response

Con este mensaje el ASN-GW confirma a la BS que ha recibido la solicitud de acceso a la red de la MS a la que está sirviendo.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	9	MS State
	OP_ID	1	OP Response
	Message Type	4	Attachment-Req
	Source Identifier	Variable	MSID
TLV		**-**	**-**

Tabla 37 Composición del mensaje MS Attachment Response

Una vez recibido este mensaje por la BS, se procede al envío de los mensajes descritos en los epígrafes 3.3.3.5.4 y 3.3.3.5.5

3.3.3.5.4 REG-RSP

Respuesta de la BS al REG-REQ. Mensaje no funcional en boc-WiMAX

Syntax	Size (bit)	Notes
REG-RSP_Message_Format() {	—	—
Management Message Type = 7	8	—
Response	8	—
TLV Encoded Information	*variable*	TLV-specific
}	—	—

Figura 34 Formato del mensaje REG-RSP

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	7	Identificador de mensaje de control
TLV		**-**	**-**

Tabla 38 Composición del mensaje REG-RSP

3.3.3.5.5 MS Attachment ACK

La BS confirma la recepción MS Attachment Response al ASN-GW mediante un ACK.

3.3.3.6 Establecimiento de conectividad IP y QoS

En esta fase la MS obtendrá finalmente conectividad a nivel red, recibirá una dirección IP y también se establecerán los SFs (Service Flows) de los que dispone así como la política QoS asociada a ellos.

Un SF es la mínima unidad de granularidad dentro de la estructura que permite ofrecer QoS. Son conexiones a nivel MAC establecidas en el interfaz R1 entre la BS y la MS. Permiten asociar a cada uno de ellos una política de QoS asociada. Para una mejor comprensión del concepto de SF ver el punto 4.3.2.

Inicialmente boc-WiMAX no contempla la posibilidad de establecer más de un SF por usuario, tampoco se encuentra habilitada la opción de incluir ningún tipo de información de QoS asociada a ese SF.

En el capítulo 4º se datallarán los procedimientos y metodologías empleadas para dotar de un módulo básico de QoS a la implemntación boc-WiMAX.

Seguidamente explicaremos las distintas fases por las que evoluciona el acceso a la red en esta etapa.

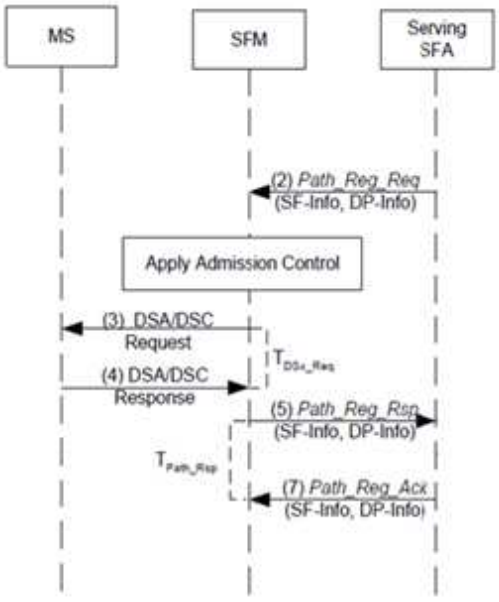


Figura 35 Fases en el establecimiento de SFs

En la figura de la derecha observamos el procedimiento que se desencadena una vez que el ASN-GW recibe el mensaje MS Attachment ACK.

En esta figura aparecen los términos SFM y SFA. Ambos son entidades lógicas, ubicadas respectivamente en la BS y el ASN-GW, encargadas de la gestión de los SFs

Como mencionamos anteriormente, el ASN-GW una vez que recibe el mensaje MS Attachment ACK procederá a crear un único SF y un data-path para la MS que solicita acceder a la red.

Los data-paths son los distintos caminos establecidos en el interfaz R6 por los que mapeamos cada uno de los SFs de los que dispone la MS.

Cada uno de los data-paths se materializa con un túnel GRE establecido entre el ASN-GW y la BS. Para una mejor compresión de los data-paths ver el punto 4.3.2

3.3.3.6.1 Path REG REQ

Este mensaje es usado para transportar la información asociada del SF con respecto al data-path creado para la MS a la que se desea otorgarle conectividad. Se genera en el ASN-GW y es transmitido a la BS.

Cada uno de los data-paths se materializa con un túnel GRE establecido entre el ASN-GW y la BS. Para una mejor compresión de los data-paths ver el punto 4.3.2

Mostramos a continuación la información enviada a la BS.

Parámetro			**Valor**	**Descripción**
Parámetros de Cabecera	**Version**		1	Versión empleada del ASN control protocol
	Function Type		3	Data Path Control
	OP_ID		1	OP Request
	Message Type		10	MS Path Reg-Req
	Source Identifier		variable	MSID
TLV			**Tipo**	**Descripción**
Registration Type			145	Initial network entry
MS Info			103	-
MS Info Sub-TLVs	**Anchor ASN GW ID**		10	Dirección IP del ASN-GW
	SF Info		185	-
	SF Info Sub-TLVs	**Reservation Action**	151	Creación
		SFID	184	Identificador de SF
		Direction	59	SF para canal de bajada

		Data Path Info		45	-
		Data Path Info Sub-TLVS	**Data-Path ID**	44	Identificador de Data Path Se usa el valor del campo key del túnel GRE creado para ese data-path

Tabla 39 Composición del mensaje Path REG REQ

Vemos como hecho resaltable como el SF creado se define de bajada. A pesar de esto, boc WiMAX usa indistintamente este SF como de bajada o subida.

3.3.3.6.2 DSA REQ

Una vez que el mensaje Path REG REQ es recibido por la BS, esta decide si se disponen de recursos suficientes en la interfaz radio para satisfacer los requerimientos de QoS de cada uno de los SF que desean ser creados. En caso afirmativo procede a crear dichos SF, almacena los parámetros asociados de cada uno (ms, SFID y data-path ID) y le asocia un valor de CID (ver punto 3.3.1.1). Finalmente procede a enviar un mensaje DSA-REQ a la MS por cada uno de los SF que pueden satisfacerse.

En este mensaje deberían ser incluidos todos los SF que se le proporcionan a la MS así como la política QoS asociada a cada uno de ellos.

Como comentamos con anterioridad, boc-WiMAX no ofrece la posibilidad de asignar parámetros de QoS a los SF por lo que sólo se enviará la MS el SFID y el CID.

Syntax	Size (bit)	Notes
DSA-REQ_Message_Format() {	—	—
Management Message Type = 11	8	—
Transaction ID	16	—
TLV Encoded Information	*variable*	TLV-specific
}	—	—

Figura 36 Formato del mensaje DSA-REQ

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	11	Identificador de mensaje de control
TLV		**Tipo**	**Descripción**
DSA REQ CID		2	Identificador de conexión asociado al SF
DSA REQ SFID		1	Identificador de SF

Tabla 40 Composición del mensaje DSA REQ

El campo Transaction ID de la cabecera del mensaje tampoco resulta implementado.

3.3.3.6.3 DSA RSP

La MS después de recibir el mensaje DSA REQ, lo procesa, construye el DSA RSP y procede a lanzar el cliente DHCP que será el encargado de solicitar una dirección IP al servidor DHCP.

Con el mensaje DSA RSP se debería confirmar la capacidad de la MS para poder gestionar el SF ofrecido con los parámetros QoS que se desea asociarle.

En boc-WiMAX este mensaje tampoco es funcional, no se confirma la aceptación del SF, simplemente se envía la respuesta vacía.

Syntax	Size (bit)	Notes
DSA-RSP_Message_Format() {	—	—
Management Message Type = 12	8	—
Transaction ID	16	—
Confirmation Code	8	—
TLV Encoded Information	*variable*	TLV-specific
}	—	—

Figura 37 Formato del mensaje DSA-RSP

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	12	Identificador de mensaje de control
TLV		**-**	**-**

Tabla 41 Composición del mensaje DSA RSP

Comprobamos como los códigos de confirmación e identificador de transacción, que deberían haberse implementado en la cabecera, no están contemplados en boc-WiMAX.

3.3.3.6.4 Path REG RSP

Con la correcta transmisión de este mensaje al ASN-GW, la BS confirma el correcto establecimiento de los SF a emplear en la comunicación BS-MS.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	3	Data Path Control
	OP_ID	1	OP Response
	Message Type	11	Path Reg Rsp
	Source Identifier	variable	MSID
TLV		**-**	**-**

Tabla 42 Composición del mensaje Path REG RSP

3.3.3.6.5 Path REG ACK

Finalmente el ASN-GW envía el ACK del mensaje Path REG RSP

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	3	Data Path Control
	OP_ID	3	OP Ack
	Message Type	11	Path Reg Rsp
	Source Identifier	variable	MSID
TLV		**-**	**-**

Tabla 43 Composición del mensaje Path REG ACK

Con este mensaje se da por finalizado el acceso a la red. Llegados a este punto la MS debería estar autenticada en la red, disponer de SF para transmitir datos con distintas políticas de QoS y disponer de una dirección IP.

3.3.4 Fases para realizar la desconexión de la MS en la red

3.3.4.1 Procedimiento de desconexión

En este punto vamos a especificar los procedimientos que incorpora la implementación boc-WiMAX para desconectar la MS de la red comparándolo con los métodos que el NWF y el estándar 802.16e proponen para realizar dicha desconexión.

El NWF establece pautas de desconexión en función de quien sea el agente que realiza el trigger para iniciar la desconexión.

Se propone un escenario en caso de ser la MS quien solicite la desconexión y otro distinto en caso de ser el ASN-GW el que propone la desconexión de dicha MS.

Boc-WiMAX sólo contempla la posibilidad de que sea la MS quién solicite la desconexión de la red. La posibilidad de que el ASN-GW inicie la desconexión de dicha MS no se encuentra implementada.

En la Figura 38 mostramos los pasos descritos por el NWF para realizar la desconexión de forma satisfactoria.

En boc-WiMAX este procedimiento resulta mucho más simplificado. En primer lugar, en la arquitectura de red desplegada para ejecutar la implementación, el serving ASN, anchor ASN y ASN authenticator son el mismo elemento. No se contempla movilidad entre ASNs. Este hecho simplifica bastante el esquema.

Tampoco se implementa un proceso de desconexión DHCP. Las direcciones IP se otorgan con una duración, transcurrido ese tiempo si la MS no envía un "alive" al servidor DHCP, este procederá a liberar esa IP para asignársela a otras MSs.

Finalmente tampoco se avisa al servidor AAA de la desconexión de la MS. Con lo cual el procedimiento de desconexión implementado en boc-WiMAX queda como se muestra a continuación

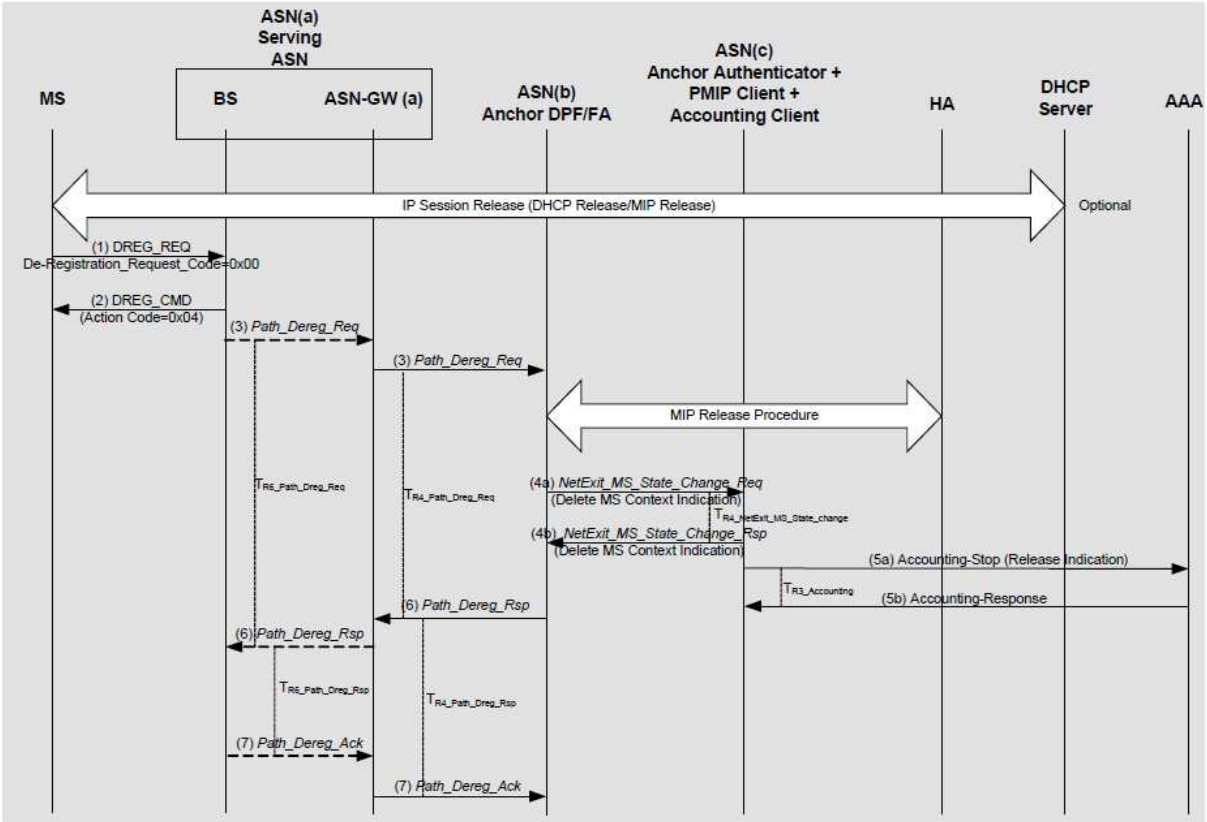
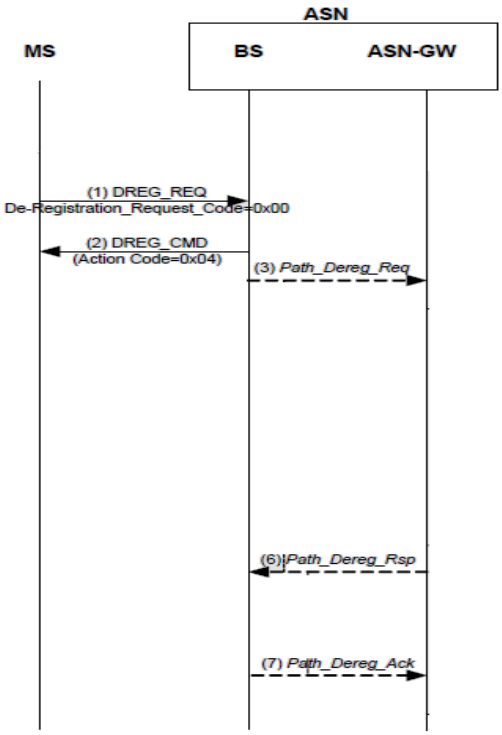


Figura 38 Fases de desconexión de la red [iniciado por la MS]

Podemos ver en la figura de la derecha como queda el procedimiento de desconexión de la MS en boc-WiMAX.

Si comparamos esta figura con la 38 comprobamos como tampoco se informa al servidor AAA de la desconexión de la MS.

A continuación pasaremos a detallar el contenido cada uno de los mensajes implementados en el network exiting de boc-WiMAX.



3.3.4.2 Mensajes implementados

3.3.4.2.1 DREG-REQ

Este mensaje se genera en la MS cuando se detecta una orden de detener su ejecución. Una vez detectada esta orden genera este mensaje para solicitar la desconexión de la red. Al ser la MS quien solicita dicha desconexión, el campo De-registration-request-code debe valer 0x00.

Syntax	Size (bit)	Notes
DREG-REQ message format() {	—	—
Management Message Type = 49	8	—
De-registration_Request_Code	8	0x00 = SS deregistration request from BS and network 0x01 = Request for MS deregistration from serving BS and initiation of MS idle mode 0x02 = Response for the Unsolicited MS deregistration initiated by the BS. 0x03 = Reject for the unsolicited DREG-CMD with action code 0x05 (idle mode request) by the BS. This code is applicable only when MS has a pending UL data to transmit. 0x04–0xFF = *Reserved*
TLV encoded parameters	*variable*	—
}	—	—

Figura 39 Formato del mensaje DREG-REQ

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	49	Identificador de mensaje de control
TLV		**-**	**-**

Tabla 44 Composición del mensaje DREG-REQ

No se implementa el campo De-registration-request-code ni ningún TLV adicional.

3.3.4.2.2 DREG-CMD

La BS transmite este mensaje hacia la MS en respuesta al mensaje DREG-REQ.

Syntax	Size (bit)	Notes
DREG-CMD_Message_Format() {	—	—
Management Message Type = 29	8	—
Action Code	8	—
TLV encoded parameters	*variable*	—
}	—	—

Figura 40 Formato del mensaje DREG-CMD

La BS debería indicar en el campo action Code la acción que debe realizar la MS. Por ejemplo cortar inmediatamente la comunicación con la actual BS, seguir escuchando a la BS pero transmitiendo solo por los CID básicos y primarios, etc.

En boc-WiMAX este mensaje no es funcional, solamente indica la recepción del DREG-REQ.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	29	Identificador de mensaje de control
TLV		**-**	**-**

Tabla 45 Composición del mensaje DREG-CMD

Cuando la MS recibe este mensaje en la implementación boc-WiMAX, procede a detener su ejecución con una llamada al sistema SIGNAL_EXIT

Una vez que la BS transmite el mensaje DREG-CMD a la MS procede a enviar el mensaje Path-DREG-REQ al ASN-GW.

3.3.4.2.3 Path DREG REQ

La BS envía este mensaje al ASN-GW a través del interfaz R6. Con el se indica al ASN-GW que la MS desea abandonar la conexión.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	3	Data Path Control
	OP_ID	1	OP Ack
	Message Type	1	Path Dreg Req
	Source Identifier	variable	MSID
TLV		**-**	**-**

Tabla 46 Composición del mensaje Path DREG-REQ

3.3.4.2.4 Path DREG RSP

El ASN-GW envía este mensaje como respuesta al Path DREG REQ. La estructura del mensaje es la misma que la mostrada en la Tabla 46 a excepción del valor Message Type. En este caso vale 2.

No se implementada ningún TLV adicional.

3.3.4.2.5 Path DREG ACK

La BS confirma al ASN-GW la recepción del mensaje Path DREG RSP mediante el envío de este mensaje. Una vez recepcionado se procede a eliminar el/los data-path asociados a la MS, eliminando sus identificadores de las tablas del ASN-GW y destruyendo el túnel GRE asociado al data-path que desea eliminar. Finalmente se elimina cualquier registro de la MS en el ASN-GW.

El mensaje sigue la misma estructura que la mostrada en la Tabla 43 cambiando el valor del campo Message Type. En esta ocasión valdrá 3.

La MS queda completamente desconectada de la red.

4 DESARROLLO Y VALIDACIÓN DEL MÓDULO QoS

4.1 Introducción

Uno de las características fundamentales del futuro *data link* AeroMACS es la de poder ofrecer distintos tipos de QoS a los distintos flujos de datos que puede generar o requerir una aeronave.

Sin entrar en grades detalles no resulta complicado entender que un avión puede generar o recibir flujos de datos provenientes de múltiples servicios. Cada uno de estos servicios no tiene por qué requerir las mismas capacidades, es decir, en función de la importancia, el tamaño, la prioridad, etc. tendrán unos requerimientos de ancho de banda y retardo distintos.

En la fase de desarrollo del *data link* AeroMACS se decidió clasificar todos los posibles servicios que puedan necesitar las aeronaves en seis categorías de servicios distintas.

- **Air Traffic Control Services (ATS o ATC).** Incluye control de tráfico aereo, servicios de información de vuelo y servicios de alerta. Esos servicios son proporcionados por ATSUs (Ait Traffic Service Units). Las comunicaciones, navegación y vigilancia en tierra y en el avión componen los servicios ATS/ATC. Definiremos tres categorias ATC; ATC1, ATC2 y ATC3.
- **Aeronautical Operation Control (AOC).** Son servicios que implican comunicaciones de datos entre el avión y el centro AOC, compañía o personal operacional del aeropuerto**.** Definiremos dos categorias; AOC1 y AOC2.
- **Network Management (NET).** Estos servicios se usan para establecer y mantener conexiones entre cada par avión-sistemas de tierra. Una única categoría.

Ya indicamos que el futuro enlace AeroMACS estará basado en la tecnología WiMAX. Por tanto, las políticas de planificación que podrán ser asociadas a cada una de las seis categorías en que podrán agruparse los distintos servicios de las aeronaves tendrán que ser las soportadas por la tecnología WiMAX. Estas políticas de planificación estarán definidas en la capa MAC.

Los tipos de planificación soportados por la tecnología WiMAX son:

- **UGS**. Diseñada para proporcionar servicios en tiempo real que transporten paquetes de tamaño fijo de forma periódica. El servicio garantiza tramas periódicas de tamaño fijo según los parámetros del flujo, reduciendo así el *overhead* y la latencia que introducen las solicitudes (Request) de las SS. Esta clase de servicio puede emplearse por ejemplo para conexiones de voz sobre IP sin supresión de silencios. Los parámetros que definen esta clase de servicio y que resultan relevantes son: mínima tasa de tráfico, máxima latencia, Jitter tolerado y tamaño de SDU (Service Data Units).
- **rtPS**. Está diseñada para soportar flujos de UL en tiempo real con paquetes periódicos de datos de tamaño variable, como sucede con el video codificado en formato MPEG. El servicio proporciona oportunidades periódicas individuales (unicast polls) para solicitar ancho de banda cumpliendo los requisitos de tiempo real, y permite a la SS especificar el tamaño deseado para el intervalo de transmisión en UL. La desventaja de este tipo de servicio es que incrementa el overhead frente a UGS para enviar las solicitudes, pero aumenta la eficiencia del transporte de datos al permitir que los intervalos de transmisión tengan tamaño variable. Los parámetros relevantes en esta clase de servicio son: Mínima Tasa de Tráfico y Máxima Latencia

- **ertPS**. Pretende aunar las ventajas de UGS y rtPS. La BS asigna intervalos de transmisión garantizados como en UGS, evitando la latencia de una solicitud de ancho de banda. Sin embargo el tamaño del intervalo de transmisión varía dinámicamente y la SS puede solicitar cambiar el tamaño del intervalo de transmisión asignado. Esta clase de servicio está diseñada para soportar tráfico en tiempo real que genere paquetes periódicos de tamaño variable, como en el caso de voz sobre IP con supresión de silencios. Los parámetros más importantes de este tipo de servicio son: Mínima Tasa de Tráfico Reservada y Máxima Latencia.
- **nrtPS**. ofrece unicast polls de forma regular, lo que asegura que el flujo de UL tenga oportunidades para transmitir solicitudes de ancho de banda incluso con la red congestionada. El parámetro más importante de esta clase de servicio de cara a este proyecto es la Mínima Tasa de Tráfico Reservada.
- **BE**. deberán solicitar intervalos de transmisión y su solicitud solo será atendida si quedan slots libres después de dar servicio a los flujos con mayor prioridad, es decir, a los flujos con QoS distinta de BE.

En la siguiente tabla especificamos la política QoS asociada a cada una de las categorías de servicio especificadas en el *data link* AeroMACS.

Categoría	ATS1	ATS2	ATS3	AOC1	AOC2	NET
QoS asociada	rtPS	rtPS	nrtPS	nrtPS	BE	rtPS

Tabla 47 QoS asociada a las categorías de servicio empleadas en AeroMACS

En las tablas 48y 49 mostramos una lista con todos los servicios requeridos por las aeronaves durante las fases de salidas o llegadas. Adicionalmente, en cada tabla se muestra en que categoría clasificamos cada uno de los servicios, el sentido de la comunicación (G = ground / A/C = airplane) y la zona del aeropuerto donde se deben ejecutar cada uno de los servicios (RAMP, GROUND y TOWER)

Operational domain execution	Service in Departure Phase		Category	Directionality
RAMP	NETCONN	Network connection	NET	G ↔ A/C
	NETKEEP	Network keep-alive	NET	G ↔ A/C
	DLL	Data Link Logon	ATC3	G ↔ A/C
	AOCDLL	Airport Operational Center Data Link Logon	AOC1	G ↔ A/C
	LOADSHT	Load Sheet Request/Transfer	AOC1	G ↔ A/C

Operational domain execution	Service in Departure Phase		Category	Directionality
	E-CHARTS	e-Charts Update	AOC2	G → A/C
	UPLIB	Update Electronic Library	AOC2	G → A/C
	SWCONF	Software configuration management	AOC2	G ↔ A/C
	SWLOAD25	Software Loading (Part 25)	AOC2	G → A/C
	SWLOAD	Software Loading	AOC2	G → A/C
	BRFCD	Aircraft Briefing Cards	AOC1	G → A/C
	ACLOG	Aircraft Technical Log Rectification	AOC1	G ↔ A/C
	TECHLOG	Technical Log Book Update	AOC1	G ↔ A/C
	AIRWORTH	Airworthiness Statement	AOC1	G → A/C
	WXTEXT	Textual Weather Report	AOC1	G ↔ A/C
	PASSENGER	Passenger Information List/Manifest	AOC1	G → A/C
	CREW-RPS	Crew rotation/planning/scheduling	AOC1	G → A/C
	CREW-BUL	Crew Briefings/Bulletins	AOC1	G → A/C
	CREW-REG	Flight Crew Recency Registration	AOC1	G ← A/C
	FLTPLAN	Flight Plan Data	AOC1	G ↔ A/C
	NOTAM	Company's Notice to Airmen	AOC1	G → A/C
	COTRAC (interactive)	Common Trajectory Coordiantion	ATC2	G ↔ A/C
	EFF	Electronic Flight Folder Exchange	AOC2	G ↔ A/C
	WXGRAPH	Graphical Weather Information	AOC1	G ↔ A/C
	CREW-L	Crew list	AOC1	G → A/C
	HANDLING	Handling process Monitoring	AOC1	G ← A/C
	CATERING	Catering inventory	AOC1	G ← A/C
	BAGGAGE	Baggage Loading	AOC1	G ↔ A/C
	NOTOC	Notice to Captain	AOC1	G → A/C

Operational domain execution	Service in Departure Phase		Category	Directionality
	LOADDOC	Load documentation Acceptance	AOC1	G ← A/C
	PREFLT-INS	Pre-Flight Inspection Signoff	AOC1	G ← A/C
	D-OTIS	Data Link Operational Terminal Information Service	ATC3	G ↔ A/C
	D-SIGMET	Data Link Significant Meteorological Information	ATC3	G ↔ A/C
	DOOR	Aircraft Door movements	AOC1	G ← A/C
	DCL	Departure clearance	ATC2	G ↔ A/C
	FLOWCON	Flow Control (CTOT & Routing)	AOC1	G ↔ A/C
	FLIPCY	Flight Plan Consistency	ATC2	G ↔ A/C
	FLIPINT	Flight Path Intent	ATC2	G ↔ A/C
	D-RVR	Data Link Runway Visual Range	ATC3	G ↔ A/C
	D-SIG	Data Link Surface Information and Guidance	ATC3	G ↔ A/C
	EFFU	Electronic Flight Folder Update	AOC2	G ↔ A/C
	TAKEOFF-CALC	Takeoff Performance Calculation	AOC1	G ↔ A/C
	D-FLUP	Data Link Flight Update	ATC3	G ↔ A/C
	PPD	Pilot preferences downlink	ATC2	G ↔ A/C
	D-TAXI	Data Link Taxi Clearance	ATC2	G ↔ A/C
	OOOI	Out-Off-On-In	AOC1	G ← A/C
GROUND	SURV	Air Traffic Control Surveillance	ATC1	G → A/C
	ACL	ATC clearance	ATC2	G ↔ A/C
	ACM	ATC Communication Management	ATC3	G ↔ A/C
TOWER	WXRT	Real Time Weather Reports for Met Office	AOC1	G ← A/C
	OOOI	Out-Off-On-In	AOC1	G ← A/C
	ACM	ATC Communication Management	ATC3	G ↔ A/C

Tabla 48 Servicios requeridos por las aeronaves (departures) [14]

Operational domain execution	Service in Arrival Phase		Category	Directionality
TOWER	OOOI	Out-Off-On-In	AOC1	G ← A/C
	NETKEEP	Network keep-alive	NET	G ↔ A/C
	AUTOLAND-REG	Autoland Registration	AOC1	G ← A/C
	ACM	ATC Communication Management	ATC3	G ↔ A/C
GROUND	SURV	Air Traffic Control Surveillance	ATC1	G → A/C
	ACL	ATC clearance	ATC2	G ↔ A/C
	D-SIG	Data Link Surface Information and Guidance	ATC3	G ↔ A/C
	D-TAXI	Data Link Taxi Clearance	ATC2	G ↔ A/C
	EFFU	Electronic Flight Folder Update	AOC2	G ↔ A/C
	FLT-JOURNAL	Flight Journal Documentation	AOC2	G ← A/C
	TECHLOG	Technical Log Book Update	AOC1	G ↔ A/C
	CREW-TIME	Flight Deck Duty Time Registration	AOC1	G ← A/C
RAMP	OOOI	Out-Off-On-In	AOC1	G ← A/C
	FOQA	Data Transfer (DFDR/QAR bulk data download)	AOC2	G ← A/C
	FLTLOG	Flight Log Transfer	AOC1	G ← A/C
	CABINLOG	Cabin Log	AOC1	G ← A/C
	ETS-REPORT	Post flight report required for ETS (Emissions Trading Scheme)	AOC1	G ← A/C
	REFUEL	Fuel ordering (Tickets) / Fuel Release	AOC1	G ← A/C
	ACM	ATC Communication Management	ATC3	G ↔ A/C

Tabla 49 Servicios requeridos por las aeronaves (arrivals) [14]

4.2 Metodología de diferenciado de tráfico

Como ya adelantamos en la introducción de este capítulo, una de las misiones fundamentales de este proyecto estaba basada en la posibilidad de contar con un simulador del *data link* AeroMACS con capacidad para diferenciar tráfico proveniente o dirigido a las aeronaves que se encuentren ubicadas en la superficie aeroportuaria.

Para realizar este simulador nos basamos en la implementación boc-WiMAX. No obstante, de la información extraída durante el capítulo 3, concluimos que dicha implementación carecía inicialmente de la capacidad de diferenciar tráfico y poder ofrecer políticas QoS asociadas.

El primer paso para añadir esta funcionalidad al simulador pasó por definir como se realizará la diferenciación del tráfico.

Para ello nos basaremos en el campo DSCP (*Differentiated Service Code Point*) de la cabecera IP de los paquetes. Cada una de las seis categorías de tráfico en las que pueden mapearse los distintos servicios requeridos por las aeronaves deben ser asociadas a un valor del campo DSCP.

El campo DSCP es una división del campo TOS (*Type of Service*) de la cabecera IPv4.

En la ilustración de la derecha observamos la estructura del campo TOS. Los seis primeros bits corresponden al campo DSCP y los dos últimos se corresponden con notificaciones de control de congestión. En boc-WiMAX usaremos tan sólo el campo DSCP para identificar a que categoría de servicio pertenece.

Una vez que boc-WiMAX obtiene el valor del campo DSCP que incorpora cada uno de los paquetes que desean ser transmitidos, procede a buscar en su base datos la política QoS asociada a ese valor DSCP y el SF que puede satisfacer esa política.

Una vez localizado el SF por el que debe enviarse el paquete se procede a transmitirlo.

4.3 Modificaciones en boc-WiMAX para soporte QoS

Para que la implementación boc-WiMAX fuera capaz de diferenciar tráfico y suministrar distintas políticas QoS a cada una de la MSs de acuerdo a las especificaciones del NWG y el estándar 802.16e fuereon necesarias una serie de modificaciones sobre la estructura inicial de dicha implementación.

4.3.1 Establecimiento de la política QoS de forma centralizada

Otro de los requerimientos del *data link* AeroMACS especificaba la necesidad de disponer de un elemento centralizado desde el cual poder definir la política QoS asociada a cada una de la MSs que deseen conectarse a la red.

Este elemento será el servidor AAA. Mas concretamente, en la implementación boc-WiMAX, el elemento desde el cual queda especificada la política QoS será el servidor *freeradius*.

En el punto 3.1 describíamos como realizar la configuración del archivo *users* del servidor *freeradius.* En este archivo debíamos establecer una entrada por cada una de las MSs que pudieran querer acceder a la red. En cada una de las entradas especificamos el secreto compartido y la MSK perteneciente a cada una de las MSs. Esta información era de vital importancia para realizar la autenticación.

Ahora deseamos introducir mas información en cada una de las entradas del archivo *users.* Aparte del secreto compartido y de la MSK, introduciremos el número de SF a los que tiene derecho la MS y la política QoS asociada a ese SF en cuestión.

La política QoS asociada a cada SF se transmite mediante el AVP 26 del protocolo del RADIUS (ver punto 3.3.3.4.5.1).

El protocolo RADIUS define el AVP con tipo 26 como un atributo sin formato en el que cada fabricante puede incluir los atributos que considere necesarios y útiles para sus implementaciones sobre RADIUS. Estos atributos dentro del AVP 26 se denominan VSA (*Vendor Specific Atributes*)

El NWF define la estructura y los distintos tipos de VSA en el stage3 [5]. Entre los muchos VSAs definidos por el WiMAX Forum nos quedaremos con el QoS-Descriptor.

Mostramos a continuación sus características

Type-ID	29 for QoS-Descriptor
Description	This attribute describes over the air QoS parameter that are associated with a flow. The QoS-Descriptor is only valid for the actual RADIUS transaction.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types are described below.

Tabla 50 Características QoS Descriptor en RADIUS

Dentro de este QoS-Descriptor pueden añadirse dentro del campo *value* una serie de TLVs de entre los expuestos en la siguiente tabla:

TLV ID	TLV Name	Length Octets
1	QoS ID	3
2	Global Service Class Name	2+6
3	Service Class Name	2+Length
4	Schedule Type	3
5	Traffic Priority	3
6	Maximum Sustained Traffic Rate	6
7	Minimum Reserved Traffic Rate	6
8	Maximum Traffic Burst	6
9	Tolerated Jitter	6
10	Maximum Latency	6
11	Reduced Resources Code	3
12	Media Flow Type	2+1
13	Unsolicited Grant Interval	4
14	SDU Size	4
15	Unsolicited Polling Interval	4
16	Media Flow Description in SDP Format	2 + Length
17	Transmission policy	1

Tabla 51 TLVs soportados dentro del QoS descriptor

Para simplificar las modificaciones sobre boc-WiMAX se decidió implementar únicamente el soporte a los TLVs QoS ID, Schedule Type, Traffic Priority y Maximum Sustained Traffic Rate.

Con estos cuatro TLVs podemos indicar a cada MS del número de SFs de los que dispone, el tipo de planificación que emplea cada uno de ellos (BE, UGS, nrtPS, rtPS y ertPS) la prioridad que tienen y la máxima tasa de tráfico sostenido permitida (en Kbps).

A continuación mostraremos las modificaciones que se suceden en los mensajes descritos en el capítulo 3 al insertar información QoS en el servidor RADIUS.

4.3.1.1 RADIUS Access-Challenge [QoS]

En el mensaje Radius-Challenge se incluye información adicional para la que boc-WiMAX no se encuentra preparado inicialmente. Si analizamos la Tabla 52 en contraposición con la Tabla 20 podemos observar como se ha incluido un VSA específico relacionado con QoS.

Por ello debieron realizarse modificaciones sobre el código fuente de la implementación boc-WiMAX para poder recibir este mensaje.

AVPs		Valor	Descripción
Vendor-Specific Atributes	**MSK**	variable	Clave de sesión maestra a partir de cual empezaremos a generar el material criptográfico necesario a emplear en el interfaz radio. Enviada después de una autenticación EAP exitosa
	QoS descriptor	variable	Conjunto de atributos (planificación, prioridad, ID y tasa máxima de tráfico sostenida) que define la política QoS de cada uno de los SF.
Message Authenticator		variable	HMAC-MD5 hash obtenido a partir del mensaje RADIUS completo y el secreto compartido entre el cliente y el servidor RADIUS.
EAP-Message		variable	Request. Contiene el EAP-Challenge obtenido mediante cifrado MD5 en base al password compartido por el cliente EAP y el servidor Radius
State		variable	Debe ser enviado de vuelta al servidor de forma inalterada

Tabla 52 AVPs codificados en el mensaje RADIUS Access-Challenge [incluyendo QoS info]

Como ejemplo mostramos en la Figura 41 un ejemplo de configuración del archivo *users* del servidor *freeradius*. En él, hemos establecido dos entradas definidas por dos MSIDs distintas 00:11:22:33:44:55 y 00:11:22:33:44:56. Para cada MS hemos definido además de la MSK que le corresponde, la política QoS asociada.

Podemos observar como a la MS 00:11:22:33:44:55 se le otorgan 4 SFs, dos con planificación nrtPS, uno con rtPS y otro BE. Adicionalmente para cada SF se establece su prioridad y su tasa máxima (en bps).

Finalmente observamos como a la MS 00:11:22:33:44:56 se le han otorgado 3 SFs, cada uno con sus parámetros QoS asociados.

En la mostramos una captura de tráfico realizada con wireshark en la que se muestra la estructura del mensaje Radius Access-Challenge. Podemos comprobar como existen cuatro AVPs tipo 26. Cada uno de ellos contiene el QoS-descriptor de cada uno de los cuatro SFs definidos para la MS 00:11:22:33:44:55.

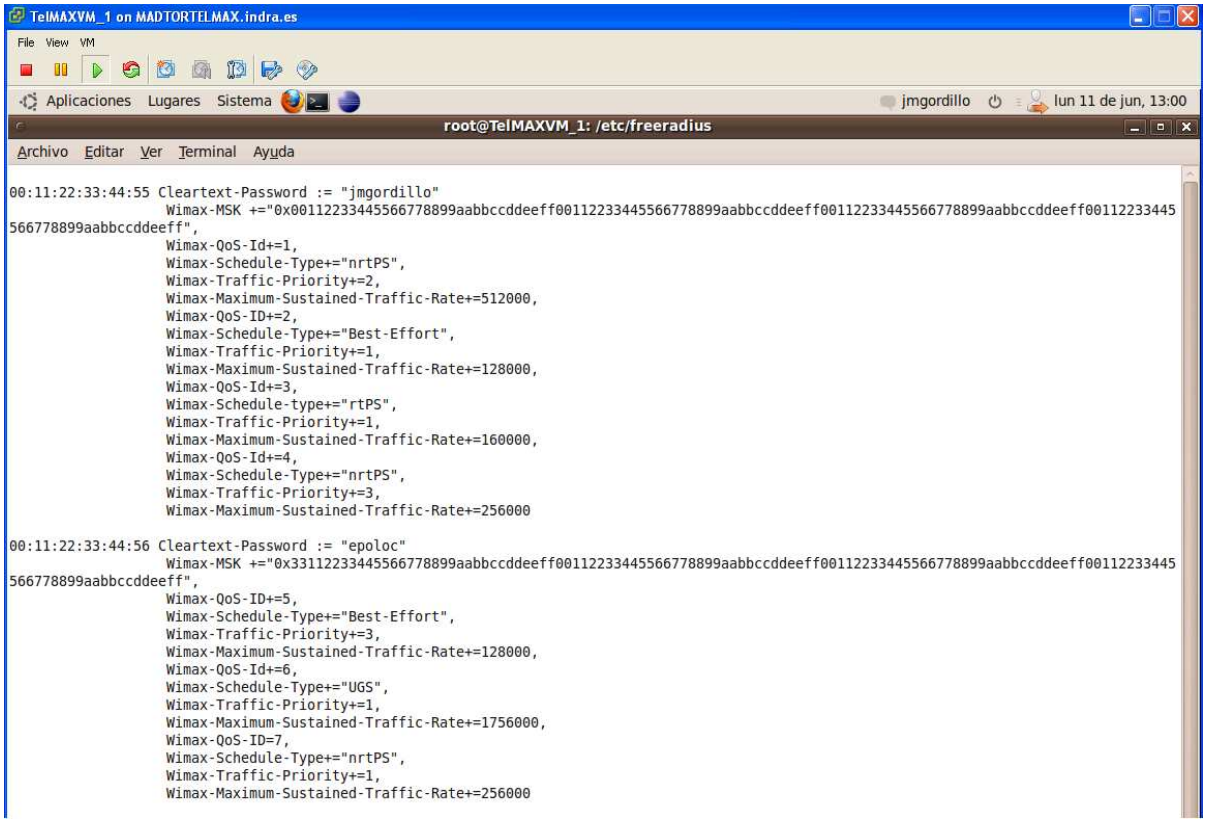


Figura 41 Ejemplo de configuración de la política QoS en el servidor freeradius

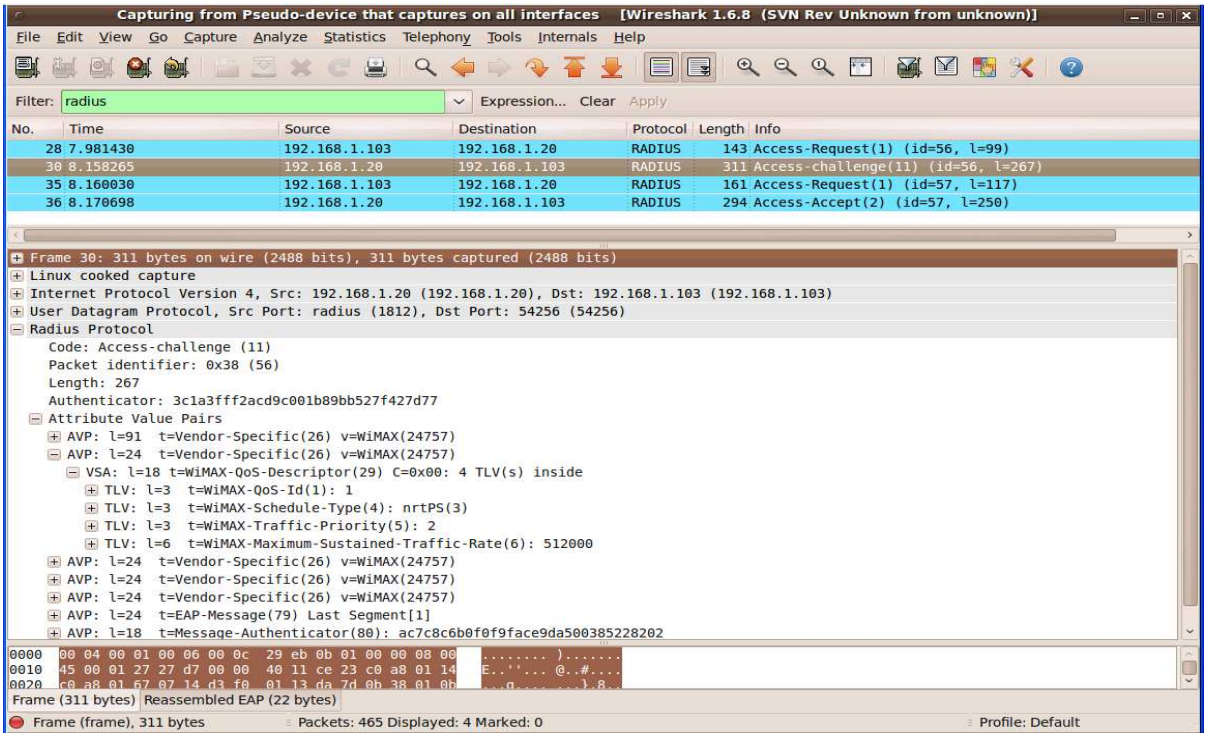


Figura 42 Captura de tráfico en el servidor RADIUS. [Mensaje Radius Access-Challenge]

4.3.1.2 RADIUS Access-Accept

Este mensaje sufre las mismas modificaciones que las mostradas en el punto 4.3.1.1 para el mensaje RADIUS Access-Challenge. Se añaden nuevamente tanto VSAs como SFs se hayan definidos para la MS que está autenticándose. Cada uno de esos VSAs contiene el QoS-descriptor de cada uno de los SF.

4.3.2 Granularidad empleada en el módulo QoS

Una vez que el servidor AAA le ha transmitido al ASN-GW el número de SF que puede usar cada MS y la política QoS asociada a cada uno de ellos, este debe proceder a crear los data-paths asociados a cada uno de los SF y transmitir a la BS la información QoS asociada a Los distintos SF que puede usar la MS.

Llegados a este punto fue necesario modificar y crear nuevas funciones en el código fuente de boc-WiMAX para permitir a la implementación soportar mas de un SF por MS y poder almacenar la información QoS de cada uno de ellos.

También fue necesario tomar una decisión de diseño importante.

Los documentos del NWG dejan abierta la granularidad que ha de tener el esquema global QoS de la red.

Cuando hablamos de granularidad nos referimos al mapeo que hacemos entre SF y data-paths.

Un data-path es un camino lógico entre el ASN-GW y la BS. Por ese camino podemos encaminar todo el tráfico con origen/destino a una misma MS o encaminar todo el tráfico que vaya a ser transmitido por uno de los SF de una MS. En las figuras 43 y 44 mostramos las dos opciones de implementación.

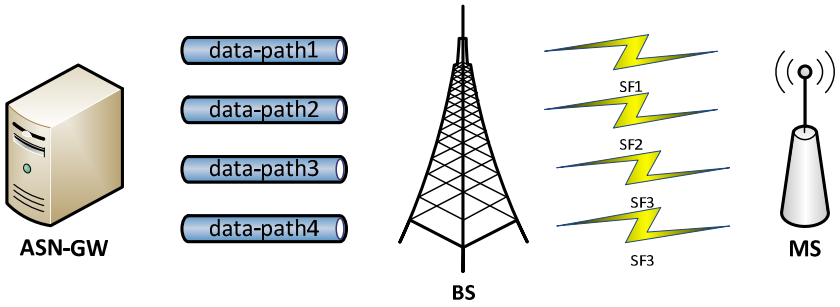


Figura 43 Granularidad QoS [data-path->SF]

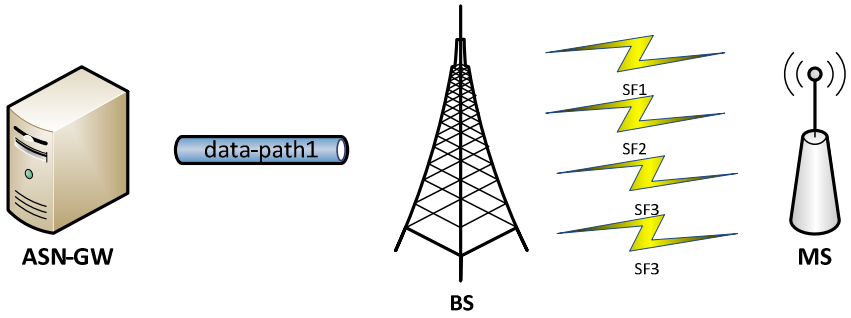


Figura 44 Granularidad QoS [data-path->MS]

Si se elige una granularidad de data-paths por SF, deberemos decidir en el mismo ASN-GW por que data-path, e indirectamente por que SF debe ir cada paquete que queramos transmitir a la MS.

Por el contrario si elegimos una granularidad de data-paths por MS, postergaremos la decisión de elegir por que SF debemos transmitir cada paquete hasta la BS.

En nuestro proyecto optamos por la segunda opción. Dejamos que sea la BS quien analice por que SF deben viajar los paquetes en función del valor DSCP que tomen, ahorrando de esta forma complejidad al ASN-GW.

Por tanto en nuestro esquema tendremos un data-path por cada MS. Debemos resaltar que también fue necesario modificar la implementación para soportar que varias MS pudieran conectarse a una misma BS ya que en un principio boc-WiMAX estaba pensado para soportar un esquema con una única BS y MS.

Para establecer el data-path, boc-WiMAX sigue las recomendaciones del NWF. Este organismo establece que los data-paths sean implementados con técnicas que permitan la tunelización IPoIP como GRE o MPLS o mediante VPNs. No obstante recomienda realizarlos con túneles GRE.

Boc-WiMAX obedece las recomendaciones del NWF y establece los data-paths como túneles GRE (Generic Routing Encapsulation) [15]. Para asignar un identificador a cada data-path (data-path ID) se hace uso del campo *key* de la cabecera del protocolo GRE. Este campo esta compuesto por 32 bits y

es usado por la BS para identificar a que MS se desea transmitir el tráfico y por el ASN-GW para identificar de que MS proviene el tráfico.

Centrándonos ahora en la granularidad en el interfaz R1, podremos disponer de uno o varios SFs entre la BS y cada una de las MSs a las que sirva. En cada uno de esos SFs podremos mapear cada una de las 6 categorías de servicio que se encuentran definidas en el *data link* AeroMACS (ver Tabla 47) y enviar a través de ellos los distintos servicios que requiera la aeronave.

En la siguiente ilustración mostramos un ejemplo de la granularidad QoS existente.

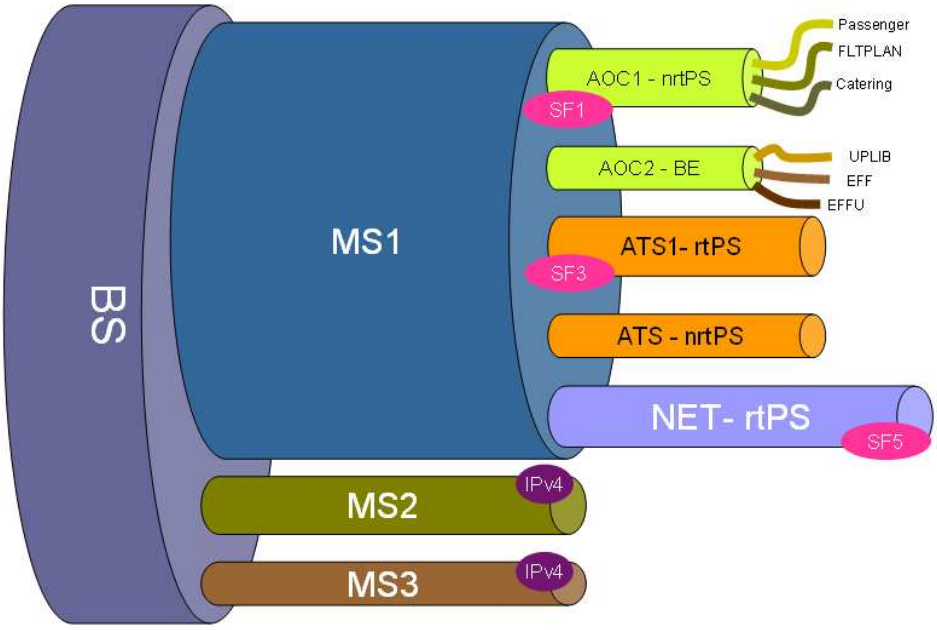


Figura 45 Granularidad QoS en el interfaz R1

4.3.3 Distribución de la política QoS a todos los elementos de la red

En el apartado 4.3.1 hemos podido comprobar como podemos definir la política QoS de forma centralizada en el servidor AAA y la forma en que podemos pasarle esa información al ASN-GW mediante el protocolo RADIUS.

Una vez que disponemos de esa información en el ASN-GW debemos procesarla y enviarsela a la BS para que esta tenga consciencia de los SFs que debe establecer con la MS y la política QoS que debe aplicar sobre cada uno de ellos.

Para transmitir esta información del ASN-GW a la BS empleamos el mensaje Path Reg-Req descrito en el apartado 3.3.3.6.1.

No obstante, deberemos modificar la estructura de los mensajes descritos en la Figura 45 para poder enviar a la BS los TLV que contengan la información de QoS.

Adicionalmente deberemos repetir el procedimiento de creación de SFs descrito en la Figura 35 tantas veces como SFs deseemos asignar a la MS.

A continuación mostramos la estructura de los mensajes que necesitaron ser modificados para dar soporte al módulo QoS.

Parámetro				Valor	Descripción
Parámetros de Cabecera	**Version**			1	Versión empleada del ASN control protocol
	Function Type			3	Data Path Control
	OP_ID			1	OP Request
	Message Type			10	MS Path Reg-Req
	Source Identifier			variable	MSID
TLV				**Tipo**	**Descripción**
Registration Type				145	Initial network entry
MS Info				103	-
MS Info Sub-TLVs	**Anchor ASN GW ID**			10	Dirección IP del ASN-GW
	SF Info			185	-
	SF Info Sub-TLVs	**Reservation Action**		151	Creación
		SFID		184	Identificador de SF
		Direction		59	SF para canal de bajada
		Data Path Info		45	-
		Data Path Info Sub-TLVS	**Data-Path ID**	44	Identificador de Data Path Se usa el valor del campo key del túnel GRE creado para ese data-path
		QoS Parameters		141	-
		QoS Parameters Sub-TLVs	**Schedule type**	variable	Tipo de planificación a emplear (BE, UGS, nrtPS, ertPS, rtPS)
			Maximun Sustained traffic rate	92	Máxima tasa sostenida de tráfico (Kbps)
			QoS priority	193	Prioridad del paquete a la hora de ser tratado en las diferentes colas

Tabla 53 Composición del mensaje Path REG REQ [incluyendo QoS info]

Cuando la BS recibe el mensaje Path REG REQ procede a crear el SF tal y como indicamos en el punto 3.3.3.6.2 con la diferencia que ahora, aparte de asociar un data-path ID, MSID y SFID, también le asociamos al SF los parámetros QoS recibidos.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Primary	Identificador de Conexión
	Management Message type	11	Identificador de mensaje de control
TLV		**Tipo**	**Descripción**
DSA REQ CID		2	Identificador de conexión asociado al SF
DSA REQ SFID		1	Identificador de SF
DSA Traffic Priority		6	Prioridad del SF
DSA Maximun Sustained Traffic Rate		7	Máxima tasa de tráfico sostenida del SF (Kbps)
DSA Scheduling Type		11	Tipo de planificación a emplear en el SF (BE, UGS, nrtPS, ertPS, rtPS)

Tabla 54 Composición del mensaje DSA REQ [incluyendo QoS]

Finalmente cuando la MS reciba el mensaje todos los mensajes DSA REQ, sabrá el número de SFs que puede usar y la política QoS asociada que se empleará en cada uno de ellos.

4.3.4 Configuración QoS en BS y MS

Durante el desarrollo del módulo QoS fue necesario modificar la implementación boc-WiMAX para gestionar la inclusión de un mayor número de parámetros configurables tanto en la MS como en la BS.

Como indicamos en el punto 4.2 la diferenciación del tráfico se realizará en base al valor del campo DSCP con el que vengan marcados los paquetes IP. En un futuro, AeroMACS deberá definir el valor DSCP con el que se marcarán los servicios que vayan a ser enviados por cada una de las 6 categorías de servicio que se han definido.

Por tanto para los SFs empleados en el canal de bajada, se introduce la posibilidad de configurar de forma manual que SF debe servir a los paquetes en función del valor DSCP con el que vengan marcados. Para ello modificamos el archivo de configuración bs.conf.

En él, introducimos el tipo de planificación y la tasa máxima de tráfico sostenida que deseamos que tengan los paquetes marcados con un valor DSCP determinado. También se introducen los parámetros QoS del SF por defecto.

Las mismas modificaciones fueron necesarias en la MS para configurar los paquetes que deben ser enviados por cada uno de los SF de subida. En este caso los parámetros configuración QoS deberán ser establecidos en el archivo ms.conf.

A continuación mostramos un ejemplo de configuración del archivo bs.conf incluyendo información QoS.

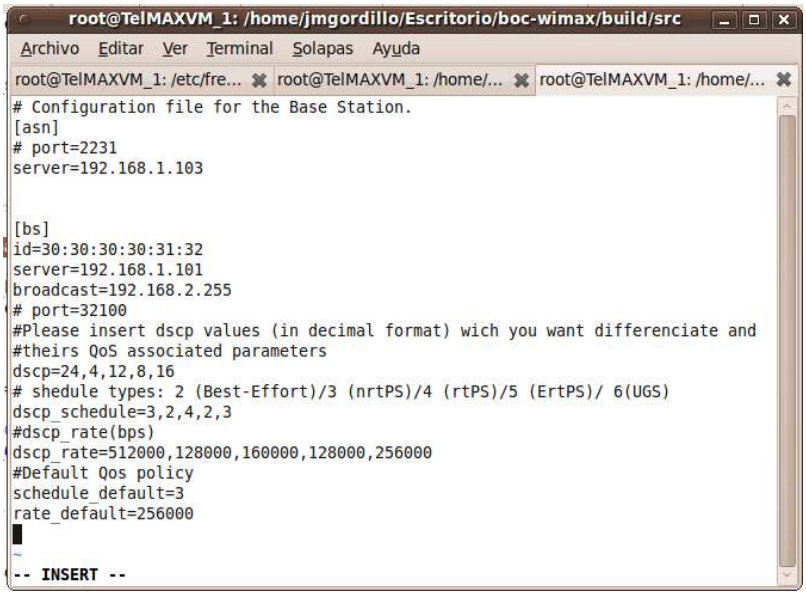


Figura 46 Ejemplo de configuración del archivo bs.conf [incluyendo QoS]

4.3.5 Funcionamiento de la arquitectura con soporte QoS

El funcionamiento del esquema QoS implementado quedaría de la siguiente manera:

a) Downlink (ASN-GW > MS)

a.1) El ASN-GW recibe tráfico desde el exterior y analiza cual es la MS destino en base a la IP destino del paquete. Una vez conocida la MS de destino busca en su base de datos el data-path ID del túnel GRE que le corresponde a la MS de destino. Finalmente procede a enviar el paquete con el túnel GRE encontrado.

a.2) La BS recibe el paquete procede a analizar el campo *key* de la cabecera del protocolo GRE y desencapsula el paquete. Obtiene el data-path ID y busca en su basa de datos la MS asociada a ese data-path ID.

a.3) Una vez que la BS conoce la MS procede a analizar el valor del campo DSCP del paquete IP que desea enviar.

a.4) Busca en su archivo de configuración si existe alguna política QoS asociada a ese valor DSCP. Si existe se busca en la base de datos si la MS dispone de algún SF que pueda satisfacer esas políticas QoS definidas en el archivo bs.conf. Si no existe ninguna política QoS en el archivo de configuración de la BS o no existe ningún SF que pueda satisfacer dichas políticas se procede a enviar el paquete por un SF establecido por defecto en el archivo de configuración.

a.5) Finalmente la BS procede a enviar el paquete por el SF encontrado en el punto a.4

b) Uplink (MS > ASN-GW)

b.1) La implementación boc-WiMAX recibe el paquete generado por capas superiores en la MS. Procede a analizar el valor del campo DSCP y busca en su archivo de configuración (ms.conf) si existe alguna política QoS asociada a ese valor DSCP.

b.2) Si la búsqueda resulta exitosa se procede a buscar si existe un SF (de los disponibles) que puede satisfacer las políticas QoS (tipo del planificación y tasa máxima de tráfico sostenida) asociadas a ese valor DSCP.

b.3) Si existe un SF que pueda satisfacer los requerimientos descritos en el apartado a.2 se procede a enviar el paquete por dicho SF. Si no existe SF o no existe una política QoS en el archivo de configuración asociada al valor DSCP del paquete IP se procede a enviar dicho paquete por el SF establecido por defecto en el archivo de configuración.

b.4) La BS recibe el paquete, procede a analizar el valor MSID que viene indicado en la cabecera MAC del paquete recibido.

b.5) Una vez que la BS obtiene el valor MSID busca en su base de datos el data-path que le corresponde y procede enviar el paquete al ASN-GW por el data-path que corresponda.

Del funcionamiento del módulo QoS concluimos:

- Podemos establecer una política QoS de forma centralizada
- Los SF definidos son los mismos tanto en downlink como en uplink
- Podemos establecer políticas QoS asociadas a los valores DSCP distintas, en downlink y uplink
- Permitimos diferenciar tráfico en base al campo DSCP de los paquetes IP
- Podemos conectar varías MSs a una misma BS

4.3.6 Uso del parámetro QoS priority

En el apartado 4.3.1 establecimos los parámetros QoS que se han definido para cada uno de los SFs. Estos parámetros son: Schedule-Type, Maximun Sustained Traffic Rate y Traffic Priority.

Hasta ahora, analizando el modo de funcionamiento del módulo QoS implementado, vimos la utilidad que presentaban los dos primeros parámetros.

En este punto describiremos la utilidad que presenta la definición de este parámetro en el módulo QoS de boc-WiMAX.

En el enlace AeroMACS se definen varios categorías de tráfico (ver Tabla 47). Observamos que existen diversas categorías de servicio llevan asociada el mismo tipo de planificación. Por ejemplo, las categorías ATS1, ATS2 y NET llevan asociada la planificación rtPS. Ante este fenómeno se desea poder disponer de un parámetro adicional que permita planificar la transmisión de paquetes, desde la BS hacia el ASN-GW o desde la BS hacia las distintas MS, pertenecientes a categorías de servicios que compartan el mismo tipo de planificación pero presenten prioridades distintas. También se podrían

establecer prioridades distintas para flujos de tráfico perteneciente a mismos tipos de planificación pero generado por MSs distintas. Podríamos priorizar el tráfico en función de la aeronave que lo genera.

Para ello creamos un algoritmo que deberá ejecutarse en la BS analizando cada uno de los paquetes que deban transmitirse hacia el ASN-GW. Conforme un paquete es entregado a boc-WiMAX para ser transmitido (ya sea en el canal de bajada o subida) el algoritmo procede a encolar el paquete en base al tipo de planificación y a la prioridad.

Para ello el planificador implementado en el algoritmo establece 5 colas distintas, una por cada tipo de planificación: rtPS, nrtPS, ertPS, UGS y BE. En cada una de estas colas los paquetes se ordenan en base a la prioridad. El primer elemento de la cola será aquel que tenga la prioridad mas baja y así sucesivamente. A su vez se permite realizar una planificación entre colas priorizando la que deseemos.

En la Figura 47 mostramos un ejemplo del ordenamiento de paquetes que puede realizar este algoritmo:

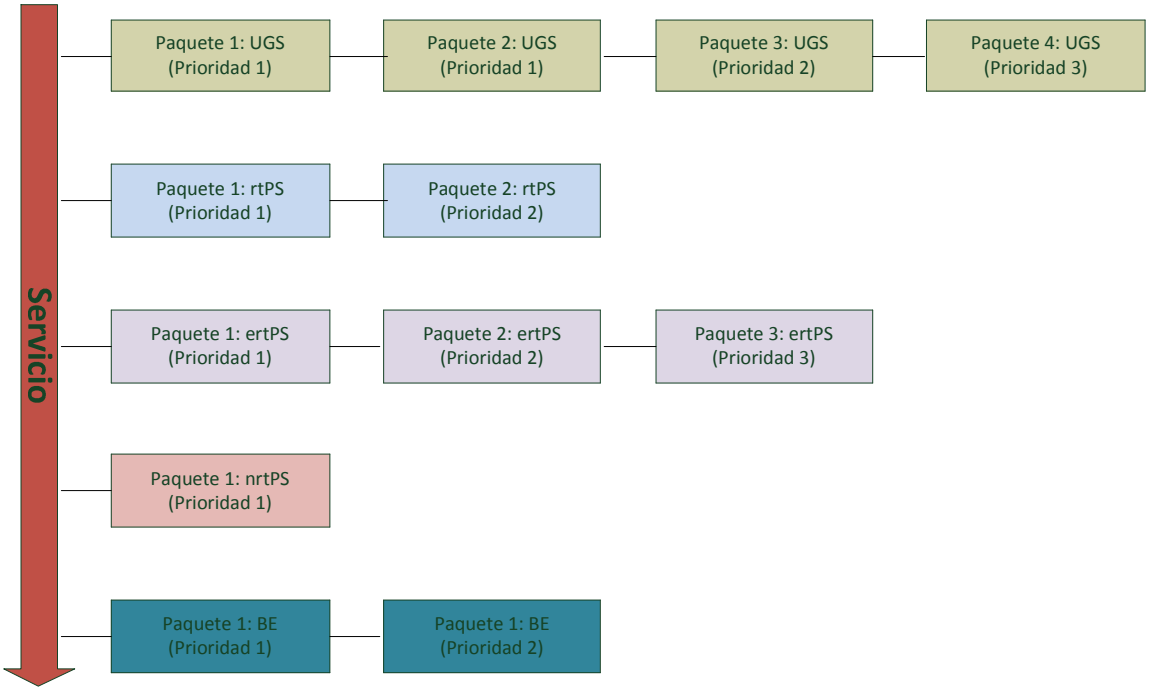


Figura 47 Ejemplo de ordenamiento basado en prioridad y tipo de planificación

Debemos destacar que a pesar de la validación de dicho planificador, en un principio esta funcionalidad no será implementada por AeroMACS puesto que se asume que debe existir la suficiente capacidad de transmisión en el interfaz R6 como para evitar cualquier congestión del enlace.

Por otro lado no se contempla de forma inicial priorizar el tráfico en función de la aeronave que lo genere.

No obstante en este punto se detalla la implementación de una funcionalidad que podría ser explotada en un futuro.

4.4 Validación del módulo QoS

En este apartado vamos a describir un caso de uso en el que podría ser usado el módulo QoS desarrollado dentro del *data link* AeroMACS. Este caso de uso también nos sirvió para validar el módulo desarrollado.

La primera tarea se concretó elaborando un escenario que pudiera asemejarse a una situación real en la que tendrá que desenvolverse el módulo QoS.

Para ello aprovechamos las nuevas funcionalidades que hemos añadido a la implementación boc-WiMAX.

Usamos dos MSs, las cuales pueden representar aeronaves circulando por un entorno aeroportuario conectadas a la red mediante el *data link* AeroMACS.

Estas MSs se conectan a la red mediante la misma BS.

Para cada una de ellas se define una política QoS de forma centralizada en el servidor RADIUS. Como podemos en la Figura 48, se definen 4 SFs para la MS1 y 3 SFs para la MS2. A cada uno de estos SFs se les asocia unos parámetros QoS. En concreto se les asocia el tipo de planificación a emplear, la tasa máxima de tráfico sostenido y una prioridad.

En cada una de las MSs se configuran los valores DSCP con los que quedarán marcados los paquetes pertenecientes a cada uno de los servicios definidos (ver tablas Tabla 48 y Tabla 49). Como ejemplo, en la MS1 se establece el valor DSCP 12 para los servicios FOCA y e-charts. Adicionalmente queda configurado el tipo de planificación Best-Effort para dicho valor DSCP.

La forma de configuración de la política QoS en las MS (canal *uplink*) y BS (canal *downlink*) nos permite asociar valores DSCP a una de las seis categorías de servicios definidas en AeroMACS (ver Tabla 47) o asignar los valores DSCP directamente a cada uno de los servicios definidos para las aeronaves.

Este hecho nos deja un gran margen de maniobra a la hora de definir la política QoS de las aeronaves ante posibles cambios en las especificaciones del *data link* AeroMACS.

Una vez definido y configurado el escenario, fue necesario implementar un algoritmo que emulara el retardo que pueden sufrir los paquetes a la hora de atravesar la interfaz radio para validar el módulo QoS.

Optamos por emplear un sencillo retardo en las funciones encargadas de enviar los paquetes, tanto en la BS como en la MS, a través del interfaz R1.

El retardo que sufren los paquetes justo antes de ser enviados es variable y se calcula de la siguiente manera:

$$t_{ret} = \frac{long_{payload}}{\max\_sustained\_traffic\_rate}$$

Es decir, para cada paquete IP que se desea enviar a través del interfaz R1 se obtiene la longitud de su *payload* y se divide por el parámetro QoS max_sustained_traffic_rate que vaya asociado al campo DSCP con el que venga marcado dicho paquete. Con esta operación obtenemos un retardo específico para cada paquete en función a su tamaño y a la política QoS con la que debe ser tratado.

Una vez que finaliza dicho retardo procedemos a enviar el paquete.

A continuación ilustramos el escenario configurado para validar el módulo QoS

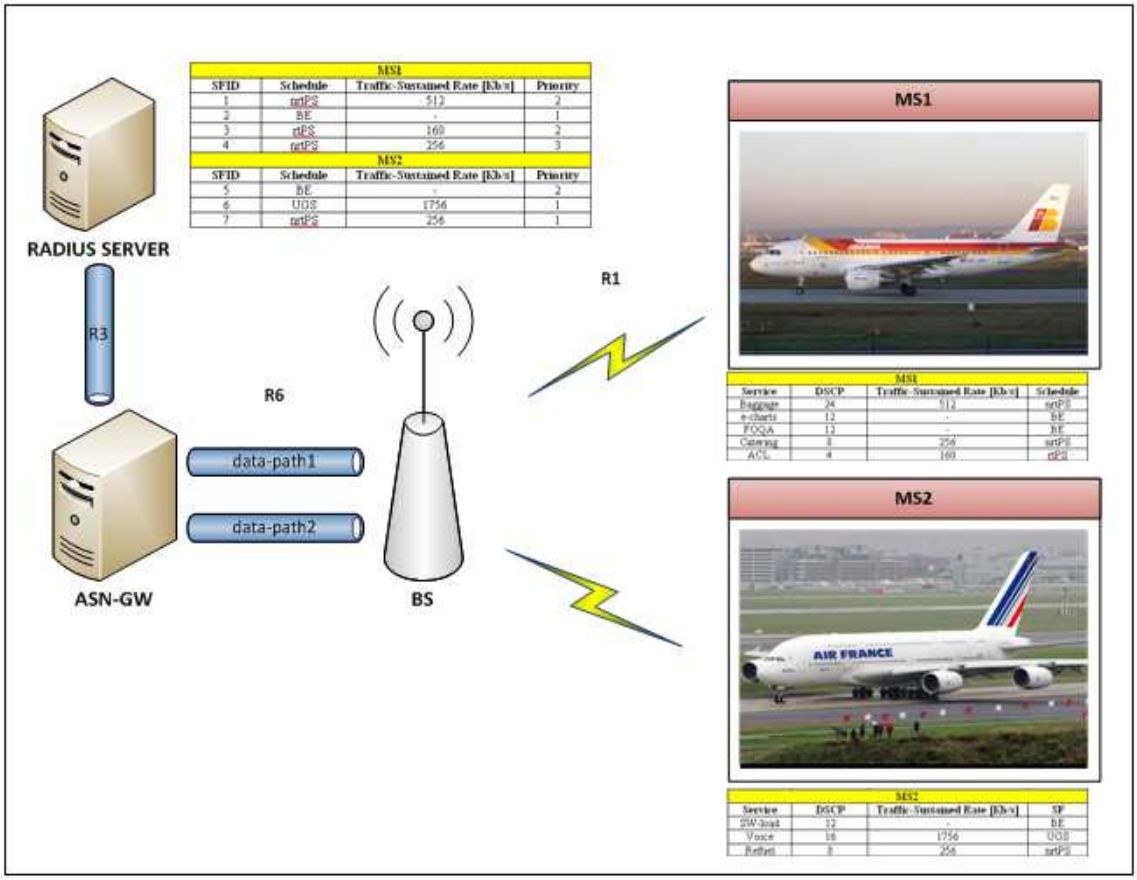


Figura 48 Caso de uso del módulo QoS

En primer lugar se verifica que efectivamente, la BS envía el tráfico proveniente de cada una de las MSs por distintos data-paths.

Para ello arrancamos cada una de las MSs, una vez que culminen el proceso *network-entry* lanzamos un ping desde cada una de las MSs hacía el ASN-GW.

Realizamos una captura de tráfico en la BS quedándonos sólo con paquetes del protocolo ICMP que vayan destinados al ASN-GW (10.20.30.2)

Mostramos los resultados de la captura en las figuras 49 y 50.

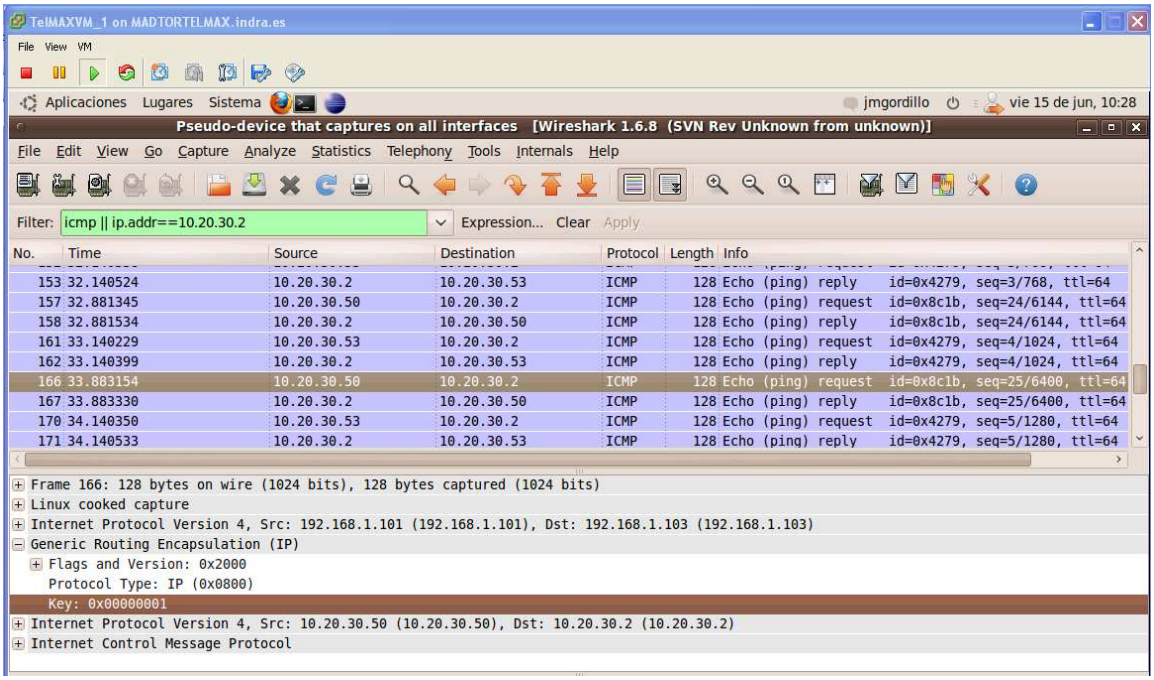


Figura 49 Captura de tráfico en la BS [ping MS1]

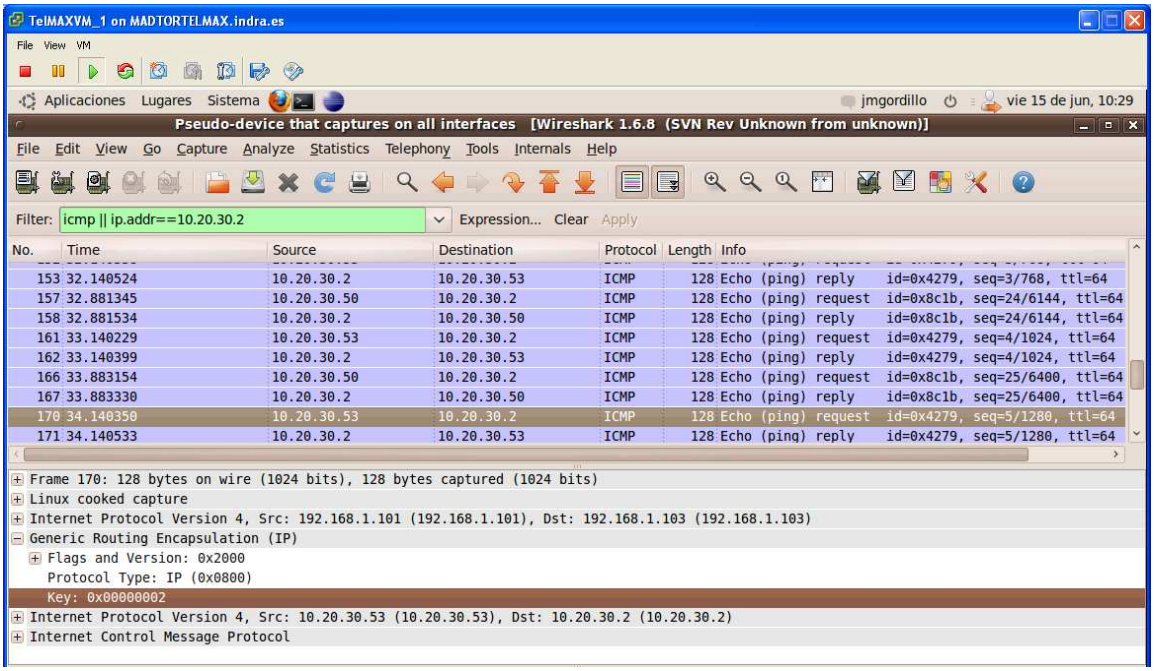


Figura 50 Captura de tráfico en la BS [ping MS2]

En la Figura 49 observamos en detalle la captura de un paquete ICMP *request* enviado desde la MS1 (10.20.30.50) hacia el ASN-GW (10.20.30.2).

En primer lugar podemos apreciar que el encapsulado GRE se está realizando con éxito, la estructura del paquete enviado a través del interfaz es la siguiente:

GRE Header | source192.168.1.101 | target 192.168.1.103 | Key: 1	IP Header | source 10.20.30.50 | target 10.20.30.2	Payload

Comprobamos como el paquete IP recibido por la MS1 se encapsula mediante el protocolo GRE y se envía por el data-path 1 (por el túnel GRE identificado por el campo key = 1)

En contraposición en la Figura 50 se muestra una captura de un paquete ICMP *request* enviado desde la MS2 (10.20.30.53) hacía el ASN-GW.

En esta ocasión la estructura del paquete reenviado de la BS al ASN-GW mediante el interfaz R6 sigue la siguiente estructura:

GRE Header | source192.168.1.101 | target 192.168.1.103 | Key: 2	IP Header | source 10.20.30.53 | target 10.20.30.2	Payload

En esta ocasión la BS procede a reenviar el paquete por el data-path 2 (túnel GRE identificado por el campo key = 2)

Una vez validada la capacidad de conectar varias MSs a través de una BS procedemos a validar el funcionamiento del módulo QoS partiendo de una configuración centralizada.

Para ello hicimos uso del software iperf. Un generador de tráfico que funciona como una aplicación cliente servidor que nos permite mediar el ancho de banda de una conexión. Además la aplicación también nos permite marcar los paquetes que genera con un valor DSCP determinado y establecer si queremos que se transporte mediante UDP o TCP.

Ejecutando el servidor del programa iperf en el ASN-GW y el cliente en la MS1 obtuvimos los siguientes resultados:

DSCP	24	08	04
Tasa (teórica) Kbps	512	256	160
Tasa (UDP-UL) Kbps	496	250	156
Tasa (TCP-UL) Kbps	489	245	154

Tabla 55 Medidas throughput para la MS1

Observando los resultados mostrados en la Tabla 55 concluimos:

- Los valores de ancho de banda obtenidos para los distintos tipos de flujos de tráfico obtenidos son muy parecidos a los establecidos teóricamente.
- Todos los anchos de banda obtenidos para los distintos flujos de tráfico son ligeramente inferiores a los definidos teóricamente por el parámetro QoS Maximum Traffic Sustained Rate. Este hecho era esperable pues las medidas se están realizando entre la MS y el ASN-GW y debemos tener en cuenta que el algoritmo empleado para simular el canal físico impone retardos producidos sólo en el interfaz R1. En la realidad se sumaran

retardos de procesamiento en la BS y en la transmisión de los paquetes en el interfaz R6 (BS/ASN-GW) lo cual hará que la tasa global disminuya ligeramente.

- Los valores obtenidos para tráfico TCP son en todos los casos ligeramente inferiores. Este fenómeno también era esperable ya que las tasas se obtienen en base al payload de los paquetes. Mientras que los *payload* de los paquetes en TCP y UDP son idénticos, TCP incluye retransmisiones lo cual empobrece ligeramente las tasas obtenidas.
- Los resultados obtenidos se muestran solamente para el canal de subida. Los resultados para el canal de bajada son idénticos al definirse la configuración QoS en la MS y en la BS de forma idéntica. Se presenta la posibilidad de usar configuraciones distintas en la BS y MS. Es decir, transmitir flujos de tráfico por un SF en el canal UL y por otro SF distinto si el canal es DL.
- Los paquetes transmitidos con la planificación BE obtienen una tasa de 125 Kbps. Aunque para este tipo de planificación no deba definirse tasa alguna ya que su espíritu se basa en coger todo el ancho de banda que pueda, en el desarrollo del módulo QoS decidimos establecer un parámetro que límite la tasa máxima con la que se puede transmitir con planificación BE. En este caso el límite se estableció en 128 Kbps.
- Comprobamos como el módulo QoS desarrollado funciona correctamente y nos permite diferenciar flujos de tráfico y aplicarle distintas políticas QoS a cada uno de ellos.

Mostramos seguidamente los resultados obtenidos para la MS2:

DSCP	16	08
Tasa (teórica) Kbps	1756	256
Tasa (UDP-UL) Kbps	1640	250
Tasa (TCP-UL) Kbps	1598	246

Tabla 56 Medidas throughput para la MS2

Las conclusiones obtenidas en las medidas de tasa para la MS2 son las mismas que las explicadas para la MS1.

5 DESARROLLO Y VALIDACIÓN DEL MÓDULO DE HANDOVER (HO)

5.1 Introducción

En este capitulo vamos a abordar el procedimiento seguido para implementar el módulo HO dentro de boc-WiMAX. Este módulo resulta fundamental en la conversión de la implementación boc-WiMAX en un simulador del *data link* AeroMACS. Debemos tener en cuenta que en un escenario real los aviones deberán trasladarse a través de la zona aeroportuaria desde que toman pista hasta que estacionan. Durante este recorrido las aeronaves serán servidas por distintas BSs por lo que resulta imprescindible abordar la construcción del módulo HO para habilitar la movilidad de las MSs.

5.2 Decisiones de diseño

En este punto vamos a detallar el escenario seguido para implementar el módulo HO. Como explicamos en capítulos anteriores, todo el desarrollo realizado sobre boc-WiMAX se ha realizado según las directrices especificados por el NWF para el perfil C WiMAX.

Como explicamos en el apartado 2.2, este perfil otorga la visión global de la red al ASN-GW. Las estaciones base no pueden comunicarse directamente entre ellas y deben hacerlo a través del ASN-GW. Este hecho resultará fundamental a la hora de realizar el módulo de handover puesto que toda la información que deban intercambiarse entre la BS origen (la que presta servicio de forma inicial a la MS) y la BS destino (BS a la que desea conectarse la MS) debe pasar a través del ASN-GW, el cual, será el encargado de retransmitir la información de una BS a otra.

El tipo HO a implementar será Hard Handover [16]. Este tipo de Handover resulta mas sencillo de implementar ya que permite que la MS permanezca desconectada un determinado tiempo de la red mientras se realiza el traspaso entre BSs. En AeroMACS se establece un tiempo máximo de 200ms para realizar el traspaso de una estación base a otra [17].

Otro aspecto importante es definir quién es el elemento de la red encargado de solicitar la petición inicial de HO que desencadenará todo el procedimiento para cambiar de BS. El NWG propone distintos escenarios en función del elemento que curse la petición (puede cursarla la MS, la BS o la red).

En nuestro desarrollo, para acomodarnos a los requerimientos del futuro *data link* AeroMACS, el encargado de cursar la petición inicial de HO será la estación móvil.

Otra decisión importante en el desarrollo del módulo es definir quien debe tomar la decisión de elegir la estación base candidata a la que migrar entre todas las posibles. Por simplicidad a la hora de realizar el emulador se decidió que fuera la MS quien eligiera la BS sobre la que realizar el HO.

En un entorno real, con la MS como elemento encargado de iniciar el HO, dicha MS debería obtener información de las capacidades que le pueden ofrecer cada una de las estaciones vecinas mediante el intercambio de mensajes específicos definidos por el estándar 802.16e[11]. Una vez que la MS dispone de la información relevante acerca de las capacidades que le pueden ofrecer cada una de las BSs tomaría una decisión óptima y cursaría la petición a su actual BS.

En nuestro caso los parámetros físicos y de capacidad referidos al interfaz R1 (aire) son obviados por lo que la MS no dispone de información útil para tomar una decisión. Por ello se decide emplear una decisión aleatoria. Para ello modificamos el código de la estación móvil para que almacene el

identificador BSID de cada una de las estaciones base vecinas. Cuando se la MS decide que debe realizar un HO selecciona la BS destino de forma aleatoria entre todas las vecinas.

Otro inconveniente de obviar totalmente los parámetros del canal radio es definir un evento determinado que sea el causante del inicio de una petición HO. En una situación real, la MS analizaría periódicamente la intensidad de la CINR (Carrier to Interference + Noise Ratio). Si esta cae por debajo de un determinado umbral se desencadenaría el procedimiento HO. Este es un ejemplo de los muchos que podríamos encontrar que nos sirve para ilustrar cual puede ser el evento detonador.

En nuestro caso, nuevamente no disponemos de información útil relevante acerca del canal radio. Por ello se decide implementar un detonador manual del proceso HO. Este detonador nos sirve para arrancar el módulo y poder validarlo. Aprovechando las mejoras realizadas para soportar el módulo QoS, decidimos aprovechar una de las nuevas funcionalidades que presenta boc-WiMAX después de este desarrollo. La funcionalidad elegida es la de poder diferenciar tráfico en función del campo DSCP de los paquetes IP. Por ello, especificamos que si la MS detecta un paquete IP con valor DSCP determinado (28) entienda que debe solicitar el inicio de un procedimiento HO.

5.3 Simulación de celdas

En todo escenario de comunicaciones móviles se debe tener en cuenta el concepto de red celular. Una red celular queda divida en celdas que son áreas centradas en torno a una estación base en la que ésta puede dar cobertura a las estaciones móviles.

Normalmente las estaciones base pueden dar cobertura en zonas que se extralimitan del área que abarca su celda. Gracias a ello las estaciones móviles pueden pasar de unas celdas a otras cambiando de estaciones bases mediante los procedimientos HO.

A la hora de implementar el módulo de HO en un entorno simulado debemos definir como simular el concepto de celda e indirectamente el de estación vecina.

Para ello, decidimos asimilar el concepto de celda en comunicaciones móviles al de subred en telemática. Como indicamos en el epígrafe 3.3.3.1, la BS emite el mensaje DL-MAP mediante un mensaje de difusión, a partir del cual se inicia el acceso a la red. Este mensaje llegará exclusivamente a los elementos que pertenezcan a la misma subred en la que se encuentra la BS.

Si deseamos introducir una segunda BS en el escenario, deberemos especificarle en su archivo de configuración una subred distinta para enviar los mensajes de difusión. De esta forma tendremos dos estaciones bases transmitiendo por subredes distintas simulando la transmisión de datos por dos estaciones bases en celdas distintas.

Finalmente también debemos simular la posibilidad de que un MS se encuentre en un a zona limítrofe entre dos celdas. Es en este aérea donde la MS tendrá conocimiento de la existencia de una o varias estaciones vecinas y donde deberá decidir si desea iniciar el procedimiento HO para migrar a otra BS. Este fenómeno se simula mediante la inclusión de nuevas interfaces de red en la MS. Es decir, si queremos que la MS detecte estaciones bases vecinas deberá disponer de tantas interfaces de red como estaciones base vecinas deseen ser detectadas. Cada una de estas interfaces de red deberán tener una IP perteneciente a la misma subred por la que está emitiendo cada una de la estaciones base. Así, se podrá recibir el mensaje DL-MAP transmitido por cada una de las BSs

Fue necesario modificar el código de boc-WiMAX encargado de manejar la recepción del mensaje DL-MAP para elaborar una lista con la direcciones IP y las BSID de todas las BS que emiten en las subredes para las que la MS presenta interfaces.

La siguiente figura ilustra el proceso de simulación. Una aeronave dentro de un aeropuerto puede pasar a lo largo de varias celdas de cobertura en función de la dimensión de su superficie. Como ejemplo el aeropuerto de Madrid-Barajas quedará dividido en 13 celdas para dar servicio al enlace AeroMACS [16]. Como indicamos anteriormente, cada celda queda definida por una subred y la MS escucha en cada una de las subredes (celdas) mediante interfaces.

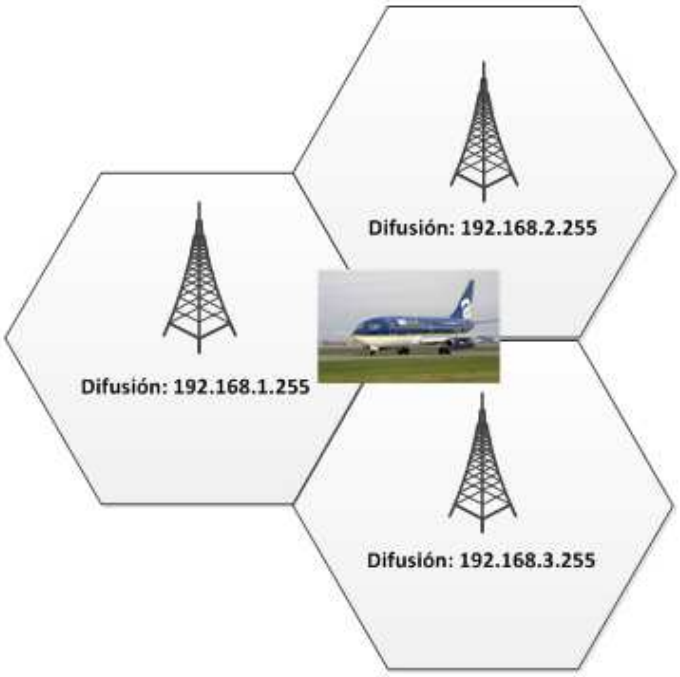


Figura 51 Simulación de celdas

5.4 Mensajes desarrollados

En este apartado vamos a describir cada uno de los mensajes que han tenido que desarrollarse para habilitar la funcionalidad HO en boc-WiMAX. Todos los mensajes se elaboran de acuerdo a las especificaciones descritas por el estándar 802.16e (para el interfaz R1) y el NWG (para el interfaz R6).

El desarrollo del módulo HO en el perfil C WiMAX se debe realizar en dos fases; fase de preparación y fase de acción. Dentro de cada una de estas fases se incluyen diversos mensajes.

5.4.1 Fase de preparación

Esta fase incluye todos los procedimientos que van desde que la MS solicita el inicio del procedimiento mediante el mensaje MOB_MSHO-REQ hasta que finalmente le es notificado a la MS la conformidad de la BS destino (*BS target* en la figura) para acogerla.

Inmediatamente después de recibir el mensaje MOB_BSHO-RSP la MS debe proceder a realizar la re-entrada a la red a través de la BS destino comenzando así la fase de acción que será descrito en el apartado 0.

A continuación mostramos una ilustración en la que se detallan todos los mensajes que deben intercambiarse entre los elementos de la arquitectura WiMAX para completar la fase de preparación. Debemos tener en cuenta que en la implementación boc-WiMAX modificada para realizar el simulador de AeroMACS, el ASN-GW de retransmisión, el Anchor ASN-GW y el ASN-GW autenticador son el mismo elemento debido a que no se contempla movilidad entre ASNs. Las fases 4 y 5 pueden realizarse en la fase de preparación o postergarse a la de acción.

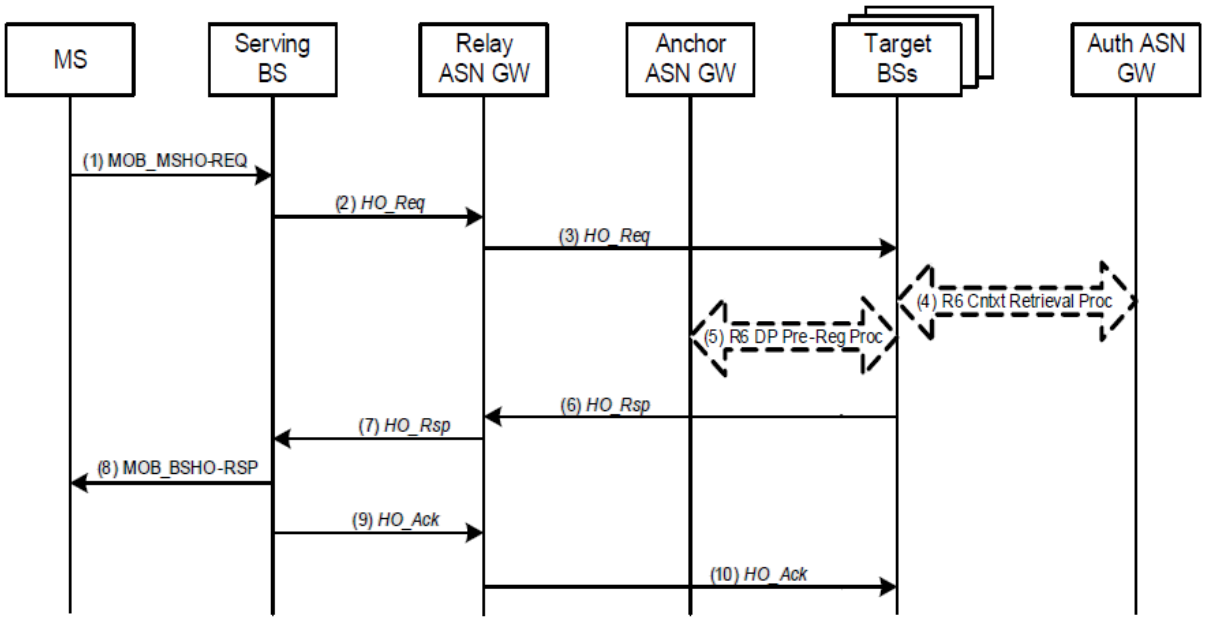


Figura 52 Fase de preparación HO

5.4.1.1 MOB_MSHO-REQ

Este mensaje se genera una vez que la MS detecta el evento definido para disparar el HO. Como indicamos en el apartado 5.2 disponemos de un disparador manual. Por tanto, una vez que la MS detecta que debe transmitir un paquete que contenga el valor 24 en su campo DSCP procede a generar el mensaje MOB_MSHO-REQ.

El objetivo de este mensaje es solicitar permiso a la BS elegida como destino para migrar hacia ella.

En este mensaje pueden transmitirse parámetros métricos (CINR, RSSI, retardo relativo, etc) de los canales de comunicación que puedan establecerse con cada una de las estaciones base que podrían prestar servicio a la MS.

En nuestro caso, se define a la MS como la encargada de decidir a que BS desea migrar. Por ello no se transmite ningún parámetro radio. Tan sólo debe incluirse en el mensaje el identificador BSID de la estación base que ha sido seleccionada como objetivo para migrar.

En la siguiente tabla mostramos la estructura del mensaje elaborado.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	57	Identificador de mensaje de control
	New BS Full	0	Número de posibles BS destino sobre las que se manda información (*).
	Neighbour BSID	variable	Identificador de la estación base seleccionada como destino
TLV		**Tipo**	**Descripción**

Tabla 57 Composición del mensaje MOB_MSHO-REQ

(*) Cuando este parámetro toma el valor 0 estamos indicando que sólo mandamos información de una BS.

5.4.1.2 HO_Req

Con este mensaje la BS origen le indica al ASN-GW que la MS desea migrar a una nueva BS.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	2	HO Control
	OP_ID	1	OP Request
	Message Type	1	HO Req
	Source Identifier	variable	MSID
TLV		**Tipo**	**Descripción**
MS Info		103	-
MS Info Sub-TLVs	**MSID**	variable	MSID
HO Type		79	Toma el valor 0 (Hard Handover)
BS Info		26	-
BS Info Sub-TLVs	**BSID**	25	Identificador de estación base
	Serving target indicator	182	Toma el valor 0. Indica que el sub-tlv BSID incluido dentro del tlv BS Info pertenece a la BS origen

BS Info		26	-
BS Info Sub-TLVs	**BSID**	25	Identificador de estación base
	Serving target indicator	182	Toma el valor 1. Indica que el sub-tlv BSID incluido dentro del tlv BS Info pertenece a la BS destino

Tabla 58 Composición del mensaje HO Req

Una vez que este mensaje es recibido en el ASN-GW, este procede a reenviarlo a la estación base destino. Debemos recordar que el ASN-GW es el único elemento que conoce la ubicación de todas las BSs presentes en la red.

5.4.1.3 Procedimiento de solicitud del contexto AK

Una vez que el mensaje HO-Req llega a la estación base destino, esta debe analizar si tiene capacidad para acoger a la nueva MS. En caso afirmativo puede proceder a solicitar el contexto AK asociado a la MS al ASN-GW o postergar esta solicitud a la fase de acción y continuar con la fase de preparación enviando el mensaje HO-Rsp al ASN-GW.

En nuestra implementación optamos por solicitar el contexto AK en la fase de preparación.

Como comentamos en el apartado 3.3.3.4.8, el contexto AK se genera a partir de la clave MSK entregada por el servidor RADIUS al ASN-GW cuando la autenticación EAP de la MS finaliza con éxito. En el HO la estación base destino solicita el contexto AK asociado a la MS al ASN-GW, evitando de esta manera tener que realizar la autenticación EAP cada vez que la MS realiza un handover.

Con este modo de funcionamiento hacemos más eficiente el procedimiento.

La solicitud del contexto AK fue implementada mediante dos mensajes tal y como establece el NWF[5].

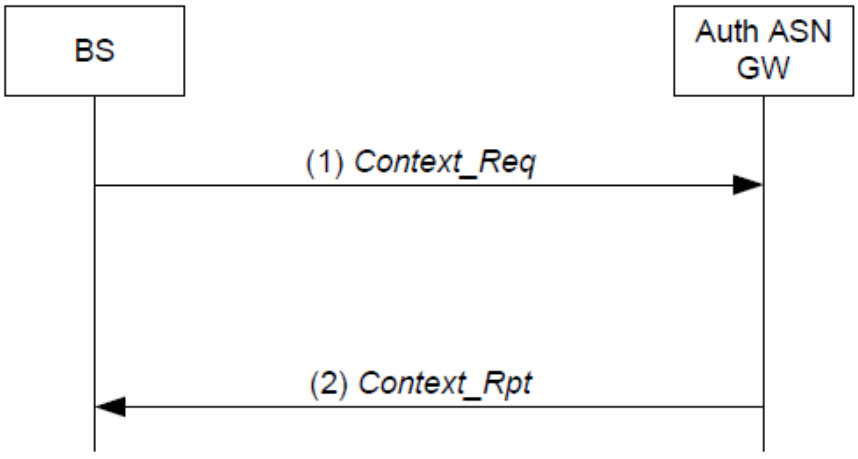


Figura 53 Procedimiento de solicitud del contexto AK durante el HO

5.4.1.3.1 Context Req

Mensaje enviado desde la estación base destino al ASN-GW solicitando el contexto AK de la MS que desea migrar hacia ella.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	4	Context Transfer
	OP_ID	1	OP Request
	Message Type	1	Context Req
	Source Identifier	variable	MSID que desea realizar el HO
TLV		**Tipo**	**Descripción**
Context Purpose Indicator		36	TLV empleado para identificar el tipo de contexto que se está solicitando. En nuestro caso se solicita el contexto AK (valor 0)
Authenticator ID		19	Dirección IP del ASN-GW encargado de autenticar a ala MS. En nuestro esquema sólo se contempla un único ASN-GW
BS Info		26	-
BS Info Sub-TLVs	**BSID**	25	Identificador de estación base
	Serving target indicator	182	Toma el valor 1. Indica que el sub-tlv BSID incluido dentro del tlv BS Info pertenece a la BS destino

Tabla 59 Composición del mensaje Context Req

5.4.1.3.2 Context Rsp

Mensaje enviado desde el ASN-GW hacia la BS destino. En él, se incluye el contexto AK solicitado.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	4	Context Transfer
	OP_ID	2	OP Rsp

		Message Type	2	Context Rsp
		Source Identifier	Variable	MSID de la MS que desea realizar el HO
TLV			**Tipo**	**Descripción**
Context Purpose Indicator			36	TLV empleado para identificar el tipo de contexto que se está solicitando. En nuestro caso se solicita el contexto AK (valor 0)
BS Info			26	-
BS Info-Sub-TLVs	**AK-Context**	**AK**	Variable	Clave 160 bits
		AK-ID	Variable	Identificador de clave 60 bits
		AK-SN	Variable	Número de secuencia de clave 4 bits
		AK-lifetime	X	Campo no funcional en boc-WiMAX
		HMAC/CMAC_KEY_U	X	Campo no funcional en boc-WiMAX

Tabla 60 Composición del mensaje Context Rsp

5.4.1.4 HO-Rsp

Una vez que la BS destino ha conseguido el contexto AK de la MS que desea migrar hacia ella, debe continuar el procedimiento HO. Este procedimiento se reanuda confirmando que la BS destino puede aceptar a la MS mediante el mensaje HO Rsp a la BS origen a través del ASN-GW.

Antes de enviar este mensaje, la BS destino genera una nueva entrada en su base de datos con la MSID de la MS que desea conectarse a ella mediante HO. Adicionalmente se creó un flag asociado a cada una de las MSIDs registradas en la BS.

Este flag (ms_reentry_flag) se activa justo después de recibir el contexto AK de la MS y previene a la BS de una solicitud de registro a la red inminente por parte de una MS que está realizando un HO.

Gracias a este *flag* podremos identificar que no se trata de un acceso a la red normal si no que estamos ante una re-entrada a la red por lo que habrá que realizar ciertas modificaciones sobre la metodología general de acceso a la red descrita en el apartado 3.3.3.

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	2	HO Control

	OP_ID	2	OP Response
	Message Type	2	HO Rsp
	Source Identifier	Variable	MSID de la MS que desea realizar el HO
TLV		**Tipo**	**Descripción**
HO Type		79	Toma el valor 0 (Hard Handover)
BS Info		26	-
BS Info Sub-TLVs	**BSID**	25	Identificador de estación base
	Serving target indicator	182	Toma el valor 0. Indica que el sub-tlv BSID incluido dentro del tlv BS Info pertenece a la BS origen
BS Info		26	**-**
BS Info Sub-TLVs	**BSID**	25	Identificador de estación base
	Serving target indicator	182	Toma el valor 1. Indica que el sub-tlv BSID incluido dentro del tlv BS Info pertenece a la BS destino

Tabla 61 Composición del mensaje HO Rsp

Este mensaje llegará al ASN-GW el cual deberá retransmitirlo a la estación base origen. Cuando dicha BS reciba el mensaje procederá a construir los mensajes MOB_BHSO-RSP y HO-Ack

5.4.1.5 HO-Ack

La BS origen genera este mensaje para confirmar a la BS destino la recepción del mensaje HO-Rsp.

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	2	HO Control
	OP_ID	3	OP ACK
	Message Type	3	HO Ack
	Source Identifier	Variable	MSID de la MS que desea realizar el HO
TLV		**Tipo**	**Descripción**

BS Info		26	-
BS Info Sub-TLVs	**BSID**	25	Identificador de estación base
	Serving target indicator	182	Toma el valor 1. Indica que el sub-tlv BSID incluido dentro del tlv BS Info pertenece a la BS destino

Tabla 62 Composición del mensaje HO Ack

5.4.1.6 MOB_BSHO-RSP

La BS origen después de recibir el mensaje HO Rsp envía este mensaje a la MS para informarle su solicitud HO ha sido aceptada y puede iniciar la re-entrada a la red a través de la BS destino.

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	50	Identificador de mensaje de control
	Neighbour BSID	variable	Identificador de la estación base seleccionada como destino
	HO-process optimization	variable	Mascara de bits usada para optimizar el procedimiento HO. Ver el punto 5.6 para mas detalles
TLV		**Tipo**	**Descripción**

Tabla 63 Composición del mensaje MOB_BSHO-RSP

Con la recepción del mensaje HO-Ack y el mensaje MOB_BSHO-RSP por parte de la estación base destino y la estación móvil respectivamente se da por concluida la fase de preparación del módulo HO.

Mostramos a continuación una captura de tráfico realizada en el ASN-GW donde podemos observar los mensajes intercambiados entre el ASN-GW y las estaciones base origen y destino durante la fase de preparación HO.

Inicialmente observamos tráfico ICMP entre la dirección IP 10.20.30.50 (correspondiente a la MS) y la dirección 10.20.30.2 (correspondiente al ASN-GW). Súbitamente activamos el disparador manual de activación HO en la MS y vemos como la recepción de tráfico ICMP en el ASN-GW se ve interrumpida y empiezan a transmitir los mensajes de la fase de preparación HO.

La dirección IP 192.168.1.123 se corresponde con la BS origen y la dirección 192.168.1.103 se corresponde con la BS destino.

Con esta captura podemos apreciar claramente la labor de retransmisión que realiza el ASN-GW en el proceso HO

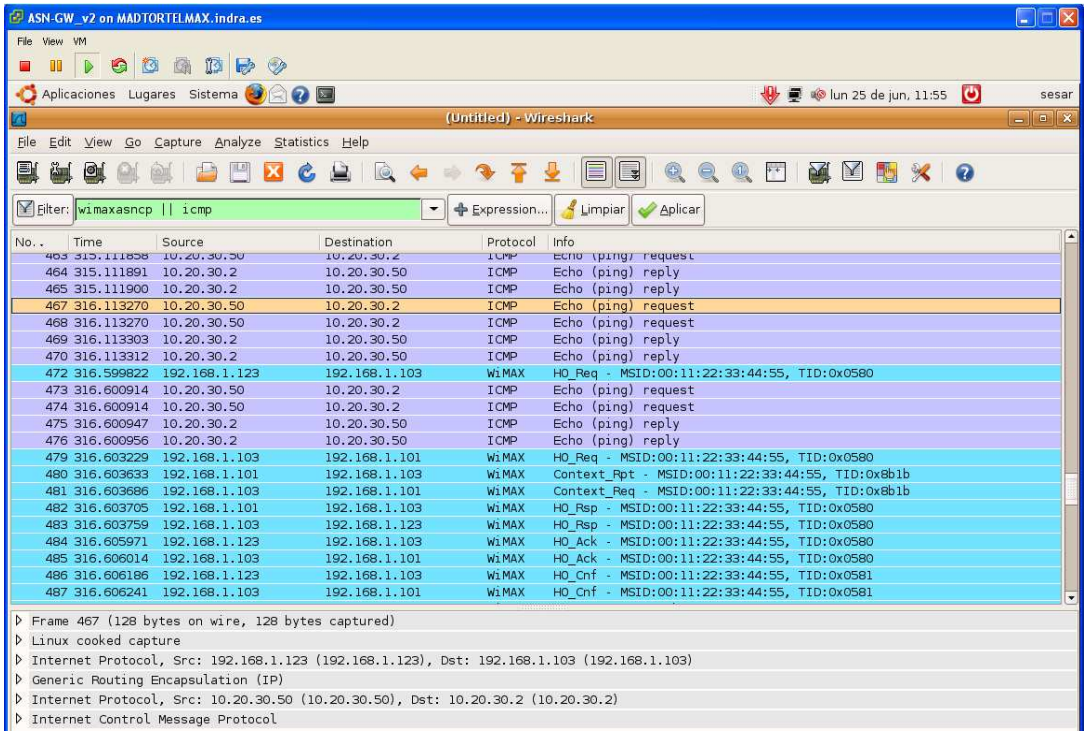


Figura 54 Intercambio de mensajes en el interfaz R6 [fase de preparación HO]

5.4.2 Fase de acción

Esta fase se inicia inmediatamente después de concluir la fase de preparación en caso de finalizar de forma exitosa.

En ella la MS inicia procede a desconectar de la BS origen e iniciar la re-entrada a la red a través de la BS destino. Cuando esta fase concluye, la MS debe recuperar la conectividad con la red.

El procedimiento implementado para completar esta fase muestra en la siguiente ilustración:

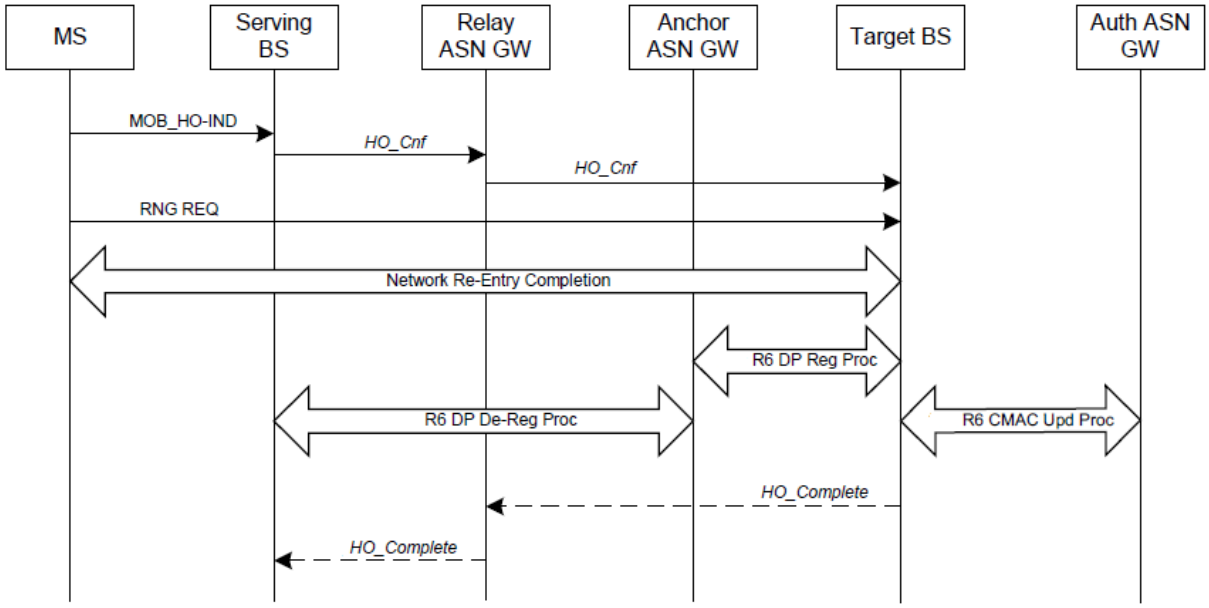


Figura 55 Fase de acción HO

Vamos a pasar a detallar la forma en la que han sido implementadas las distintas etapas que componen esta fase.

5.4.2.1 MOB_HO-IND

Con este mensaje se inicia la fase de acción HO. Antes de ser enviado la MS activa el reentry_flag creada ex profeso para el módulo HO. Se transmite de la MS a la estación base origen.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	59	Identificador de mensaje de control
	Mode	variable	Toma el valor 0 indicando que la acción a realizar es un HO
	HO-IND type	variable	Toma el valor 0 indicando que la acción que se desea realizar es desconectarse de la BS origen
	Target BSID	variable	Identificador de la BS destino a la que se desea migrar
TLV		**Tipo**	**Descripción**

Tabla 64 Composición del mensaje MOB_HO-IND

5.4.2.2 HO Cnf

Cuando la BS recibe el mensaje MOB_HO-IND procede a confirmar a la BS destino que el HO ha sido aceptado por todas las partes y la MS comenzará la re-entrada a la red a través de ella. Debemos tener en cuenta que muchos de los mensajes que hemos implementado tanto en la fase de preparación como en la de acción pueden perderse o no llegar a su destino a tiempo. Es por ello que todos los procedimientos deben ser confirmados en sus distintas partes.

Parámetro		Valor	Descripción
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	2	HO Control
	OP_ID	4	OP Indication
	Message Type	3	HO Cnf
	Source Identifier	Variable	MSID de la MS que desea realizar el HO
TLV		**Tipo**	**Descripción**
BS Info		26	-
BS Info Sub-TLVs	**BSID**	25	Identificador de estación base
	Serving target indicator	182	Toma el valor 0. Indica que el sub-tlv BSID incluido dentro del tlv BS Info pertenece a la BS origen
BS Info		26	**-**
BS Info Sub-TLVs	**BSID**	25	Identificador de estación base
	Serving target indicator	182	Toma el valor 1. Indica que el sub-tlv BSID incluido dentro del tlv BS Info pertenece a la BS destino

Tabla 65 Composición del mensaje HO Cnf

5.4.2.3 Re-entrada a la red vía BS destino

Una vez enviado el mensaje MOB_HO-IND, la MS procede a iniciar el registro a la red con la nueva BS enviándole el mensaje RNG REQ. Una vez llegados a este punto comenzaríamos a recorrer las etapas descritas en el apartado 3.3.3 con ligeras modificaciones.

La estructura de este mensaje no sufre ninguna alteración con respecto a la mostrada en la Tabla 8 Composición del mensaje RNG-REQ en boc-WiMAX.

La BS destino recibirá el mensaje RNG-REQ y procederá a enviar el mensaje RNG-RSP.

Al detectar la BS que estamos ante un proceso de re-entrada procederá añadir el TLV HO_PROCESS_OPTIMIZATION en el que se incluyen las fases del proceso de entrada a la red que deben omitirse. La estructura del mensaje quedará de la siguiente manera:

Parámetro		Valor	Descripción
Parámetros de Cabecera	**CID**	Basic	Identificador de Conexión
	Management Message type	5	Identificador de mensaje de control
TLV		**Tipo**	**Descripción**
Basic CID		Variable	Número de identificador de conexión básico. Ver apartado 3.3.1.1
Primary Management CID		Variable	Número de identificador de conexión primario. Ver apartado 3.3.1.1
HO Process Optimization		Variable	Ver apartado 5.6

Tabla 66 Composición del mensaje RNG-RSP [re-entrada a la red tras HO]

La MS almacenará los datos correspondientes a la optimización HO y procederá a enviar el mensaje SBC-REQ siguiendo la estructura mostrada en la tabla 3.3.3.3.1.

La BS recibirá dicho mensaje y procederá a iniciar la fase “Preattachment” enviando el mensaje MS_Preattachment-Req al ASN-GW. Este mensaje presentará el formato descrito en la tabla 3.3.3.3.2.

Cuando este mensaje llegue al ASN-GW y se detecte que estamos ante una re-entrada se procederá a actualizar todos los datos de la MS en la base de datos del ASN-GW. Tendremos que actualizar todos los datos referentes a la BS usada para darle servicio.

Seguidamente procederemos a enviar el mensaje MS_Preattachmente-RSP hacia la BS siguiendo la estructura mostrada en la tabla 3.3.3.3.3.

La BS comprobará el valor del re-entry flag. Si está activo, estaremos ante un acceso a la red después de un HO. En esta situación, por motivos de eficiencia no debemos volver a realizar la autenticación EAP de la MS. Tengamos en cuenta que la BS destino ya ha obtenido el contexto AK de la MS durante la fase de preparación HO.

Por tanto, todos los mensajes descritos en el tema 3 referentes al procedimiento de autenticación EAP transmitidos entre el servidor RADIUS y la MS y los mensajes “Key Change Directive” destinados a pasar el contexto AK desde el ASN-GW hacia la BS deberán ser omitidos.

Después de esta breve explicación podemos entender que la BS después recibir el mensaje MS_Preattachmente-RSP procederá a generar los mensajes SBC-RSP y MS_Preattachment-Ack, tal y como se hace en el acceso normal a la red, y adicionalmente deberá enviar seguidamente el mensaje TEK-Challenge (ver 3.3.3.4.10) a la MS saltándose todos los pasos de autenticación EAP.

Desde este punto, el acceso a la red continúa de forma normal, hasta la fase de establecimiento de conexión.

En un acceso a la red inicial, una vez recibido el mensaje DSA-REQ en la MS, se procedería a lanzar el cliente DCHP para obtener una dirección IP y con ello conectividad a nivel de red.

No obstante, en una re-entrada a la red no resulta necesario volver a solicitar una dirección IP puesto que ya disponemos de ella. Adicionalmente AeroMACS establece que la dirección IP de las MSs no debe cambiar durante el procedimiento HO [17].

Por tanto fue necesario modificar el código fuente en la MS para no lanzar nuevamente el cliente DHCP en caso de estar realizando una re-entrada a la red.

Mostramos finalmente es el esquema a seguir para completar un acceso a la red después de un HO.

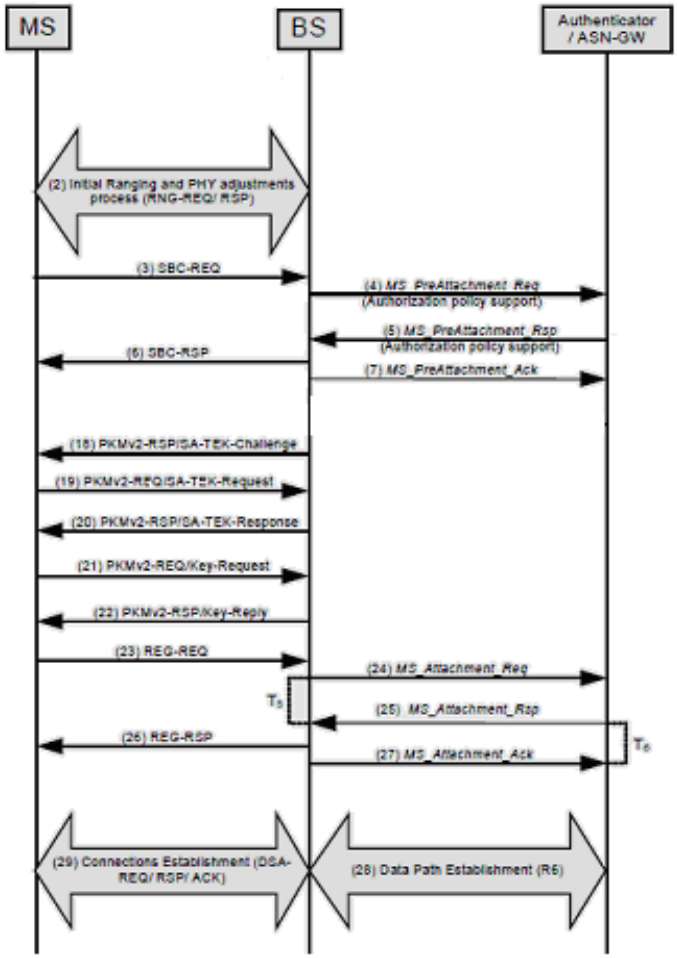


Figura 56 Re-entrada a la red después de un HO

5.4.3 Desconexión con la BS origen

La desconexión implica eliminar el data-path establecido entre el ASN-GW y la BS origen, todos los SFs establecidos entre la BS origen y la MS y la eliminación de toda la información asociada a la MS en la BS origen.

Para conseguir estos objetivos fue necesario modificar y crear código fuente nuevo que fue integrado en boc-WiMAX.

5.4.3.1 Eliminación de data-path

Una vez recibido en el ASN-GW el mensaje MS_Attachment-Ack se comprueba si estamos ante un acceso normal a la red o un acceso tras HO. En caso de encontrarnos ante una re-entrada el ASN-GW procede a eliminar el data-path establecido entre él y la BS origen que servía a la MS que ha realizado el HO.

Para ello se elimina el túnel GRE que soportaba dicho data-path. Posteriormente con la recepción del mensaje Data-Path REG-REQ el ASN-GW procederá actualizar toda la información referente a los SFs que disponía la MS en la BS origen con los que dispondrá en la BS destino.

En el módulo desarrollado no se contemplan variaciones referentes a los SFs al realizar un HO. Es decir, todos los SF que la MS disponía en su antigua BS deben ser aceptados por la nueva.

5.4.3.2 Eliminación de SFs con la BS origen

Una vez finalizado el proceso de re-entrada a la red descrito en el apartado 5.4.2.3, la MS vuelve a estar conectada a la red mediante una BS distinta. Sin embargo aún falta un paso para terminar el procedimiento HO.

La BS destino una vez recibido el mensaje Path_Reg-REQ procederá a construir el mensaje HO_Complete para enviárselo a la BS origen. El objetivo de este mensaje es indicar a la BS origen que la MS migró con éxito a una nueva BS y puede proceder a eliminar toda la información asociada a ella y destruir los SFs que mantenía con dicha MS.

La estructura del mensaje HO_Complete se muestra en la siguiente tabla.

Parámetro		**Valor**	**Descripción**
Parámetros de Cabecera	**Version**	1	Versión empleada del ASN control protocol
	Function Type	2	HO Control
	OP_ID	4	OP Indication
	Message Type	5	HO Complete
	Source Identifier	Variable	MSID de la MS que desea realizar el HO
TLV		**Tipo**	**Descripción**
Result Code		154	Código de resulta de acción. Si el procedimiento resulta exitoso toma valor 0.

Tabla 67 Composición del mensaje HO Complete

5.5 Validación del módulo HO

Una vez que tuvimos desarrollado el módulo HO procedimos a validarlo. Para ello se configuró el escenario de red avanzado descrito en el epígrafe 2.4.2.

Una vez montado el escenario y puesto en funcionamiento todos los actores involucrados, se procedió a enviar un ping desde la MS1 (10.20.30.50) hacia el ASN-GW (10.20.30.2). Durante el transcurso del envío de tráfico ICMP desde la MS1 al ASN-GW procedimos a disparar manualmente el procedimiento de HO con la generación en la MS de un paquete IP marcado con el valor 28 en el campo DSCP tal y como se describe en el epígrafe 5.2.

Como era de esperar una vez que la MS detecta que debe transmitir un paquete IP con valor DSCP igual a 28 procede iniciar el procedimiento HO con el envío del mensaje MOB_MSHO-REQ.

En la Figura 57 podemos ver como en el ASN-GW se captura el tráfico ICMP preveniente de la MS1. En los campos resaltados en rojo observamos como el tráfico proveniente de la MS1 (10.20.30.50) le está llegando a través de la BS1 (192.168.1.123) a través del túnel GRE2.

De repente vemos como en la captura se interrumpe el número de secuencia de los paquetes y nos aparecen 4 paquetes de respuesta a los ICMP-REQ transmitidos por la MS que no han podido ser entregados al destino (MS). Esto es debido a que se ha activado el procedimiento de Hard HO y la comunicación con la MS ha quedado interrumpida durante un cierto instante mientras se realiza el traspaso entre BSs.

Finalmente en la Figura 58 vemos como una vez superado el procedimiento HO los paquetes ICMP-REQ vuelven a recibirse en el ASN-GW y lo paquetes ICMP-RSP pueden entregarse al destino de nuevo. Sin embargo en esta ocasión los paquetes dirigidos o transmitidos por la MS1 pasan a través de la BS2 (192.168.1.101) mediante el túnel GRE1.

Por tanto el módulo HO funcionalmente funciona correctamente.

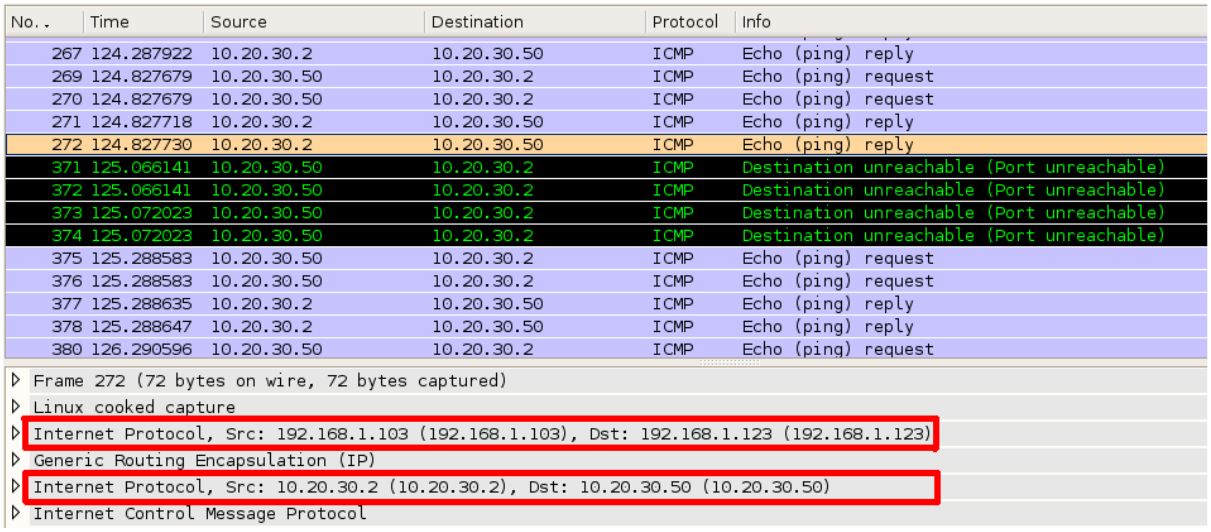


Figura 57 Captura de tráfico ICMP en el ASN-GW [antes de iniciar HO]

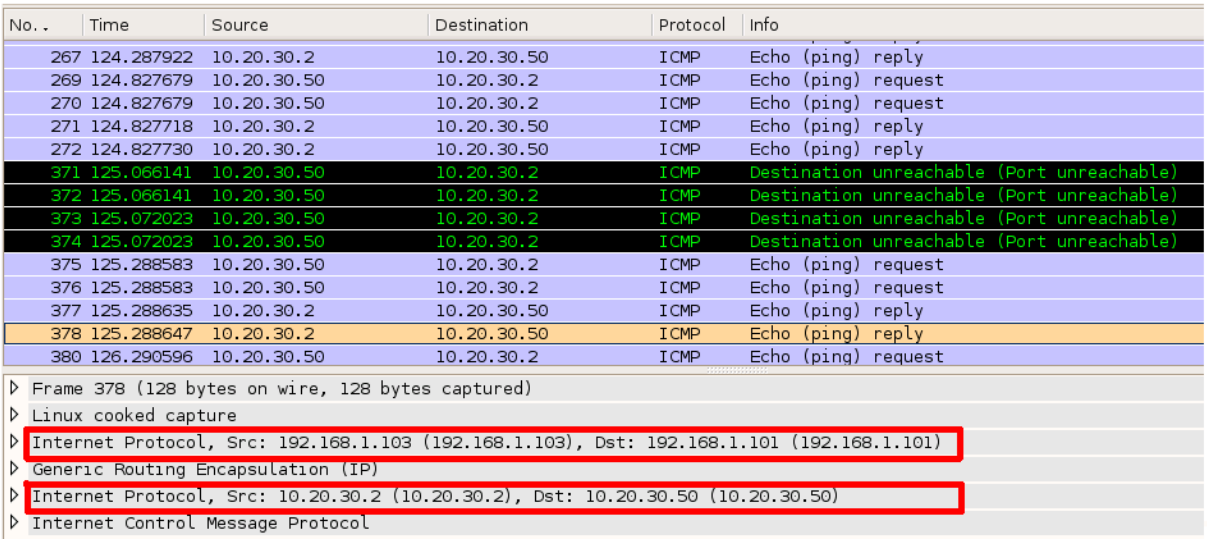


Figura 58 Captura de tráfico ICMP en el ASN-GW [después de iniciar HO]

5.6 Optimización HO

A lo largo del capítulo 5º hemos expuesto la metodología desarrollada para poder implementar el módulo HO. Durante el desarrollo del módulo hemos descritos los pasos para que una estación móvil pueda cambiar de una estación base a otra de acuerdo a las directrices descritas por el NWF y el estándar 802.16e.

En este epígrafe queremos resaltar otra de las funcionalidades implementadas en este módulo. El estándar 802.16e propone mecanismos que pueden ser usados para optimizar el proceso de HO reduciendo el tiempo de traspaso entre BSs. Dependiendo de los requerimientos de la arquitectura que se desee desplegar puede resultar útil hacer uso de estos mecanismos.

Mas concretamente, el estándar propone optimizar el proceso eliminando determinadas fases del proceso de re-entrada a la red tras un HO (ver Figura 56).

Para conseguir esta optimización, debemos hacer uso del TLV “HO Proccess Optimization”.

Este TLV es enviado desde la estación destino a la MS en el mensaje RNG-RSP. También puede ser enviado mediante el mensaje MOB_BSHO-RSP.

Hemos implementado las dos opciones. Sin embargo, a la hora de validar el módulo preferimos considerar funcional la primera de las opciones. En ella es la BS destino quién establece la política de optimización a seguir.

A continuación vamos a mostrar el significado que presenta el TLV “HO Proccess Optimization”.

Bit	Significado (0 = inactivo // 1 = activo)
0	Se omiten los mensajes de gestión SBC-REQ/RSP durante el proceso de re-entrada
1	Se omite toda la fase PKM durante el proceso de re-entrada a excepción de la subfase TEK
2	Se omite la subfase TEK englobada dentro de la fase PKM
3	Se deshabilita la opción de solicitar una nueva dirección IP después de finalizar el proceso de re-entrada

4	Se omiten los mensajes de gestión de adquisición de la hora y día
5	Se omiten los mensajes de gestión TFTP durante el proceso de re-entrada a la red
6	Se establecen los distintos contextos establecidos en la MS como estáticos
7	Se omiten los mensajes de gestión REG-REQ/RSP durante el proceso de re-entrada

Tabla 68 Significado del TLV "HO Proccess Optimization"

En el módulo HO desarrollado sólo se considera la posibilidad de alterar de forma conjunta los bits 1 y 2. Es decir, podemos configurar el procedimiento de re-entrada a la red eliminando toda la fase PKM. El resto de opciones no se consideran de utilidad para el futuro data link AeroMACS y no se encuentran implementadas en boc-WiMAX.

El procedimiento de re-entrada a la red con la optimización HO activada quedaría de la siguiente manera:

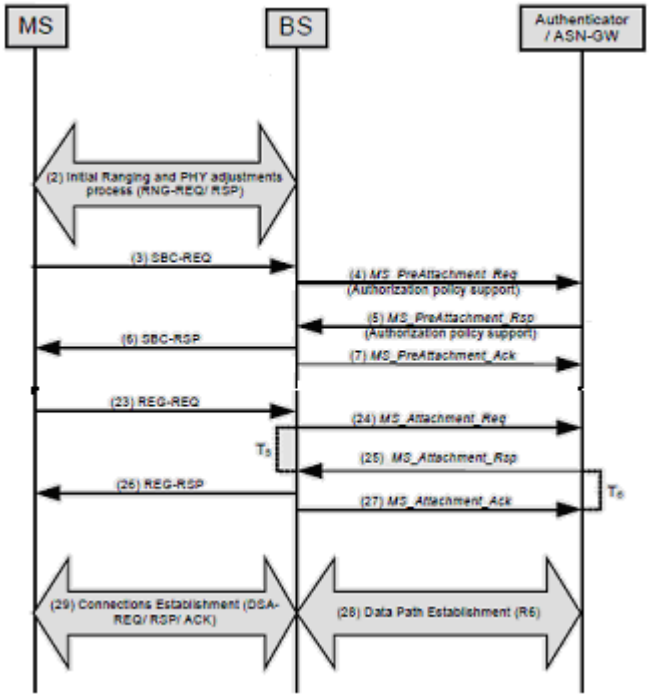


Figura 59 re-entrada a la red tras HO [optimización activada]

La activación de la optimización se debe configurar de forma manual en la estación destino mediante el archivo de configuración ms.conf.

Para ello hemos introducido un nuevo campo dentro de dicho archivo de configuración que deberemos establecer a 1 si deseamos activar la optimización o dejarlo a cero para realizar una re-entrada completa a la red.

Mostramos seguidamente el aspecto que presenta el archivo de configuración ms.conf después de todas las modificaciones realizadas sobre él para soportar los módulos QoS y HO.

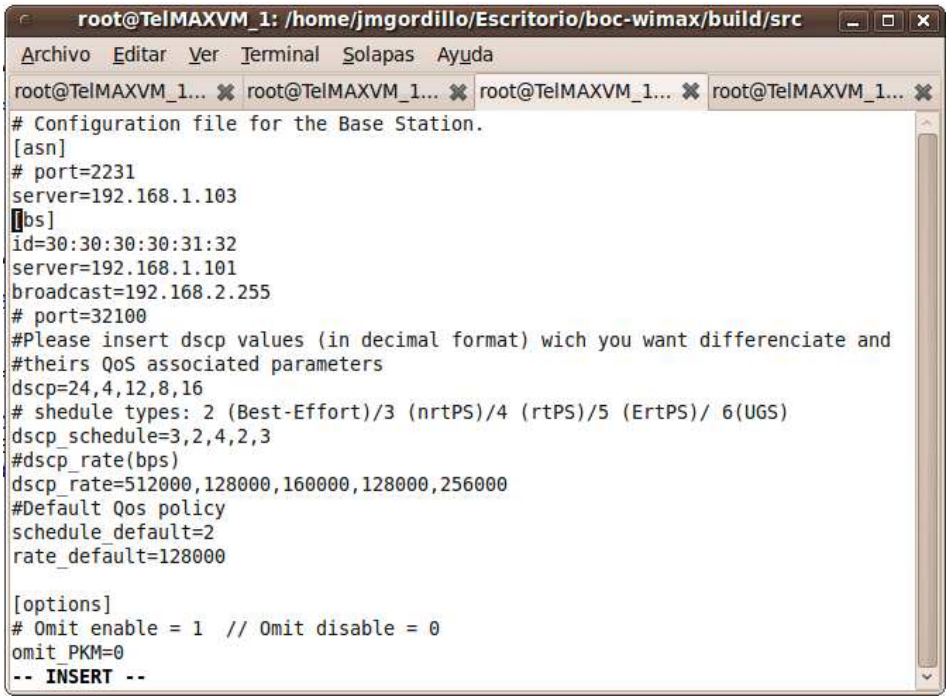


Figura 60 Archivo de configuración ms.conf [configuración HO & QoS incluida]

Debemos tener en cuenta que al deshabilitar el procedimiento PKM estamos prescindiendo de todos los procedimientos de seguridad pensados para intercambiar y actualizar el material criptográfico. Las consideraciones de seguridad que versan sobre este hecho quedan fuera del ámbito de este proyecto, no obstante debemos resaltar el que el enlace AeroMACS está pensado para funcionar en entornos aeroportuarios, los cuales son entornos muy restringidos y controlados. Por ellos muchos de los posibles elementos a considerar que puedan amenazar la seguridad durante el procedimiento de HO deben ser ponderados en su justa medida.

Finalmente exponemos en la siguiente tabla una comparativa del tiempo que tarda en completarse el proceso de HO con la optimización activada y desactivada.

Duración proceso HO AeroMACS	Duración proceso HO	Duración proceso HO optimizado
<200 ms	91.82 ms	81.04 ms

Tabla 69 Comparativa de tiempos [módulo HO]

Estas cifras representan el tiempo medio transcurrido en milisegundos desde que la MS recibe el disparador para iniciar el HO hasta que concluye el proceso de re-entrada a la red con la recepción del mensaje DSA-REQ en dicha MS.

Como era de esperar, el módulo HO requiere menos tiempo en completarse con la optimización activada. No obstante, tanto con la optimización activada como sin ella, los requerimientos de tiempo HO para el *data link* AeroMACS son conseguidos.

6 CONCLUSIONES Y LÍNEAS FUTURAS

A lo largo de esta memoria hemos ido detallando cada uno de los pasos seguidos para incorporar los módulos de Handover y QoS a una implementación WiMAX, pensada inicialmente para dar servicio a usuarios fijos y sin funcionalidad para ofertar distintas calidades de servicio.

Partiendo de una implementación WiMAX basada en el estándar 802.16, hemos conseguido sentar las bases para evolucionar está implementación a una versión capaz de soportar usuarios móviles basándonos en el estándar 802.16e del IEEE y en las recomendaciones del NWG. Para ello, hemos desarrollado un módulo básico de Handover desarrollado en C++ capaz de permitir hard-handover. Antes de poder insertar este nuevo módulo, fue necesario modificar la implementación original para que ésta pudiera dar servicio a varias estaciones base y móviles a la vez.

El módulo quedó validado, después de su desarrollo, mediante un caso de uso en el que una estación móvil era traspasada de una estación base a otra de forma virtual.

También quedó implementado y validado un procedimiento especial de Handover (fast-Handover), el cual, permite un traspaso entre estaciones base de forma más rápida.

Finalmente quedo implementado un módulo básico de QoS capaz de ofrecer distintas calidades de servicio a través de una misma conexión. Para ello se hizo uso del concepto de flujo de servicio especificado en el estándar WiMAX 802.16e. Con dicho módulo se permite diferenciar el tráfico IP en función de su campo DSCP aplicándole distintas políticas de transmisión. También quedó habilitada la posibilidad de definir distintas políticas de transmisión en función de la estación móvil que desee transmitir y del sentido de la transmisión (ascendente o descendente)

Este módulo también quedó validado mediante un caso de uso.

Por tanto, conseguimos aproximar una implementación WiMAX básica a los requerimientos que necesita el radioenlace AeroMACS para prestar servicio a las aeronaves que se encuentren en superficies aeroportuarias.

No obstante, para que esta implementación pueda finalmente convertirse en un prototipo aún deben desarrollarse y depurarse muchos módulos. Entre las principales carencias se encuentra la adaptación de esta implementación a una política de seguridad basada en certificados mediante tecnología RSA. Esta evolución es necesaria puesto que la implementación actual utiliza algoritmos de cifrado basado en MD5, los cuales resultan muy vulnerables para ser usados en comunicaciones tan críticas.

También queda mucho por hacer en todo lo que respecta a la interfaz WiMAX R1 (radio). Como hemos comentado durante el proyecto, esta interfaz ha sido simulada y simplificada al máximo para poder elaborar nuestros módulos en unas condiciones mínimas como para poder validarlos.

En definitiva este proyecto sólo trata de ser una pequeña piedra dentro del proyecto SESAR que revolucionará en un futuro muy próximo las comunicaciones aeronáuticas dentro de nuestro continente.

7 ESTUDIO ECONÓMICO DEL PROYECTO

Este anexo final presenta el coste relativo exclusivamente al trabajo realizado y presentado en esta memoria, sin tener en cuenta otro tipo de costes asociados como por ejemplo el coste de los equipos de red, acceso instalación. Por lo tanto, se detalla el coste del estudio, a nivel personal.

El proyecto tuvo una duración de un año y tres meses, fue desarrollado en las instalaciones de Indra Sistemas en Torrejón de Ardoz. Dicha empresa sufragó todo el material necesario para realizar dicho proyecto a través de fondos europeos, así como los emolumentos del personal implicado, a excepción del tutor de la universidad.

En primer lugar, debemos indicar que el proyecto se realizó en su totalidad utilizando software libre o gratuito. En la siguiente tabla mostramos el listado de las aplicaciones empleadas.

Utilidad	Denominación
Sistema Operativo	Ubuntu
Implementación WiMAX	Boc-WiMAX
Virtualización	Vsphere
Compilador	IDE C++ Eclipse
Servidor/Cliente DHCP	Dnsmasq
Servidor AAA	Freeradius
Configuración túneles	Open VPN
Analizador de tráfico	Wireshark
Mediciones Throughput	NS2

Tabla 70 Software Empleado

Como gastos imputables deberíamos incluir el uso del CPD de Indra, la amortización del equipo ofimático empleado y los gastos prorrateados de comunicaciones, luz, agua y mantenimiento de las instalaciones durante el año y tres meses que duró el proyecto.

A este gasto le asignaremos una cuantía de 60 euros mensuales.

También deberemos asumir el coste de amortización del equipo informático empleado. En este proyecto se hizo uso de un portátil DELL valorado en 1000 €. Asumiendo una depreciación del 20% anual para este tipo de materiales de consumo, obtenemos un coste por amortización de 250 € calculados para los 15 meses que duró el proyecto.

Por otro lado tendremos que asumir los gastos de personal. Por el desarrollo de dicho proyecto percibí una beca de 750 euros mensuales por jornadas de 5 horas.

Adicionalmente dispuse de la ayuda de dos tutores. Uno en la empresa y otro en la universidad. Para calcular el gasto en honorarios para los tutores se dispone del dato orientativo publicado por el colegio

oficial de ingenieros de telecomunicaciones en años anteriores. El COIT establecía unos honorarios orientativos de 75 €/hora para un ingeniero senior.

En este tipo de proyectos se suele asignar un 7% del total de las horas empleadas a la labor de los tutores. Teniendo en cuenta que el proyecto se elaboró en jornadas de 5 horas de lunes a viernes durante 15 meses, obtenemos un total de 1500 horas.

Así calcularemos los honorarios de los tutores como: 1500 horas*0.07*75 €/hora = 7875 €

Concepto	Coste	Cantidad	Total
Entorno de Trabajo	60 €/mes	15 meses	900 €
Equipo Informático	250 €	1	250 €
Ingniero de Proyecto	750 €/mes	15 meses	11,250 €
Director de Proyecto [1]	7%	112,500 €	7,875 €
Director de Proyecto [2]	7%	112,500 €	7,875 €
Total sin IVA			28,150 €
Total IVA (21%)			34,061.5 €

Tabla 71 Coste económico del proyecto

8 ABREVIATURAS Y ACRÓNIMOS

AAA	↔	Authentication, Autorizaction & Account / Autenticación, autorización y contabilidad
AK	↔	Authorization Key / Clave de autorización
AOC	↔	Aeronautical Operation Control / Control de operaciones aeronauticas
ASN-GW	↔	Access Service Network Gateway / Pasarela de acceso a los servicios de red
ATC	↔	Air Traffic Control / Control de tráfico aéreo
ATM	↔	Air Traffic Management / Gestión de tráfico aéreo
AVP	↔	Atribute Value Pair / Dupla atributo-valor
BS	↔	Base Station / Estación base
CHAP	↔	Challenge Handshake Authentication Protocol / Protocolo de autenticación por desafio mutuo
CID	↔	Connection Identifier / Identificador de conexión
CINR	↔	Carrier to Interference plus Noise Ratio / Relación portadora a ruido más interferencia
CMAC	↔	Cipher based Message Authentication Code / Clave basada en código de autenticación del mensaje
CNS	↔	Communication, Navigation & Surveillance / Comunicación, navegación y vigilancia
CSN	↔	Connectivity Service Network / Servicio de conexión de red
CPE	↔	Customer Premises Equipment / Equipo local de cliente
DHCP	↔	Dynamic Host Service Provider / Huesped dinámico proveedor de servicios
DSCP	↔	Differentiated Service Code Point / Punto de servicios de codificación diferenciados
GNSS	↔	Global Navigation Satellite System / Sistema global de navegación por satélite
GRE	↔	Generic Routing Encapsulation / Enapsulación de enrutado genérica
HA	↔	Home Agent / Agente propio
HMAC	↔	Hash based Message Authentication Code / Hash basado en el código de autenticación de mensaje
HO	↔	Handover / Traspaso
MS	↔	Mobile Station / Estación móvil
MSK	↔	Master Session Key / Clave maestra de sesión

NAI	↔	Network Access Identifier / Identificador de acceso a la red
NSP	↔	Network Service Porvider / Proveedor de servicios de red
NWF	↔	Network WiMAX Forum / Foro WiMAX de red
OFDM	↔	Orthogonal Frecuency Division Multiplexing / Multiplexado por división de frecuencias ortogonales
PMK	↔	Pairwise Master Key / Clave maestra dual
QoS	↔	Qualtiy of Service / Calidad de servicio
RRM	↔	Radio Resource Management / Gestión de recursos radio
RSSI	↔	Received Signal Strength Indication / Indicator de potencia de la señal recibida
SA	↔	Security Association / Asociación de seguridad
SF	↔	Service Flow / Flujo de tráfico
SESAR	↔	Single European Sky ATM Research / Investigación para la gestión del tráfico aéreo europeo en un espacio aéreo unificado
TOS	↔	Type Of Service / Clase de servicio
WiMAX	↔	Worldwide Interoperability for Microvawe Access / Interoperabilidad mundial mediante acceso por microondas
WP	↔	Working Package / Paquete de trabajo

REFERENCIAS

[1].- http://www.sesarju.eu/

[2].- Release 1 (NWG) WiMAX network architecture

[3].- http://www.thekelleys.org.uk/dnsmasq/doc.html

[4].- http://tools.ietf.org/html/rfc3046

[5].- WiMAX Forum Network Architecture, Release 1.0 – Stage 3 (*Detailed Protocols and Procedures*)

[6].- http://freeradius.org/

[7].- http://www.vmware.com/es/virtualization/

[8].- Future Aeronautical Communications, *Edited by Simon Plass, Institute of Communications and Navigation, German Aerospace Center (DLR), Germany , ISBN 978-953-307-625-6*

[9].- http://opensource.bolloretelecom.eu/projects/boc-WiMAX/

[10].- *The MD5 message-Digest Algorithm*, RFC 1321

[11].- IEEE 802.16e, *Air Interface for fixed and mobile broadband wireless access systems*

[12].- RFC 3748, Extensible Authentication Protocol. http://tools.ietf.org/html/rfc3748

[13].- RFC 2865, Remote Authentication Dial in User Service (RADIUS), http://www.ietf.org/rfc/rfc2865

[14].- SESAR 15.2.7 WA2, AeroMACS Traffic modelling_v1.0.doc

[15].- RFC 2784, Generic Routing Encapsulation

[16].- D04_AeroMACS_Deployment_and_Integration

[17].- 15.2.7. WA1 "AeroMACS SRD"